Redefining Information Operations

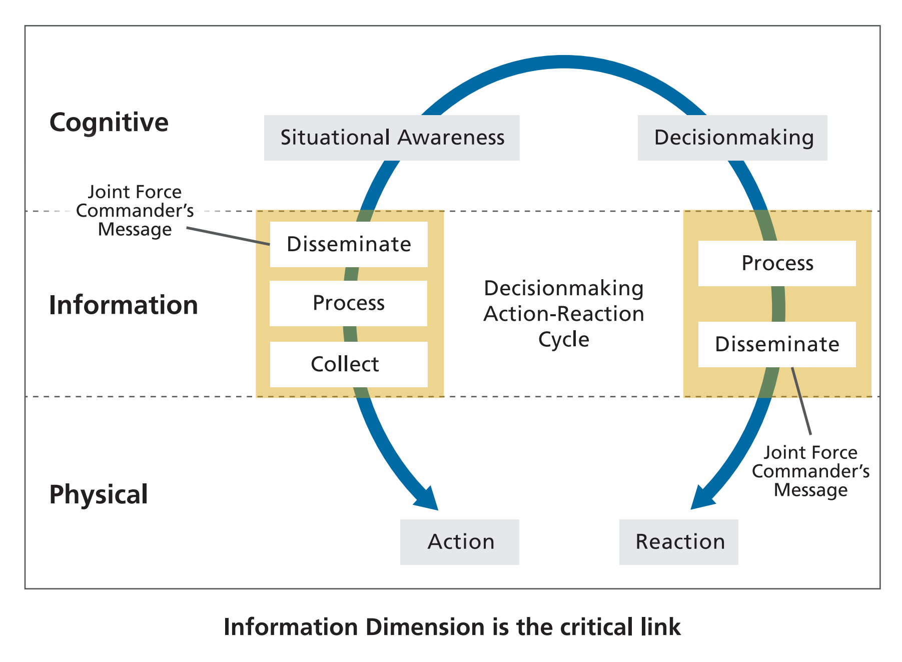
By CARMINE CICALESE

Whether it is strategic communication, information operations, or cyberspace operations, the Department of Defense (DOD) recognizes the importance of conducting operations within the information environment. Over the past decade, several information-related capabilities have grown or matured revealing that the military recognizes the value of conducting operations in the information environment.

Computer network operations have expanded to cyberspace operations, and the Services have established cyberspace component commands to complement U.S. Cyber Command.[1] Military information support operations forces have also matured as the U.S. Army Special Operations Command has established the Military Information Support Command and added another group-level command.[2] The Air Force continues to increase the number of behavioral influence analysts, integrating them into joint commands.[3] In August 2012, the Joint Forces Staff College hosted the Office of the Secretary of Defense–sponsored Information Environment Advanced Analyst Course to further develop the military's ability to analyze and operate in the information environment.

To capture the power of information, DOD must recognize the value in understanding the information environment and articulating the integrating processes required within information operations. Despite continued misunderstanding and rewording, information operations is an important integrating function for achieving the commander's objectives through the information environment—a complex and dynamic environment depicted by human interaction with other humans, machines, and subsequent cognitive determinations or decisions. This information environment further comprises three interlocking dimensions—physical, information, and cognitive—that are interwoven within a decisionmaking cycle (see figure 1). This article uses historical vignettes to offer greater clarity in understanding the difference between strategic communications and information operations and adding depth in recognizing how military information-related capabilities affect the decisionmaking process.

Figure 1. Decisionmaking Cycle: Dimensions Are Linked


Cognitive
Situational Awareness
Decisionmaking
Joint Force Commander's Message
Disseminate
Process
Collect
Information
Decisionmaking Action-Reaction Cycle
Process
Disseminate
Joint Force Commander's Message
Physical
Action
Reaction
Information Dimension is the critical link

The New War of Words

A Secretary of Defense memorandum signed January 25, 2011, stresses the importance of strategic communication (SC) and information operations (IO) in countering violent extremist organizations, while also redefining IO for DOD and subsequently the joint force. As Dennis Murphy noted on mastering information, "The U.S. military will achieve such mastery by getting the doctrine right."[4] The Secretary's memorandum was a step in the right direction leading to recent doctrinal changes. *Joint IO* is now defined as the "integrated employment, during military operations, of information-related capabilities in concert with other lines of operations to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own."[5]

This new definition detaches itself from a reliance on the previously included core capabilities of computer network operations, operations security, and military information support operations—previously known as psychological operations, electronic warfare, and military deception. This change should benefit the force. First, it allows the commander and staff to consider more options for affecting decisionmaking than simply relying upon the previously stated capabilities. Simultaneously, it allows capabilities to grow and change unencumbered by a doctrinal or fiduciary connection to IO. Lastly, the new definition recognizes the ability of the commander to affect adversary and potential adversary decisionmaking. All the while, IO remains an integration function, not a

Colonel Carmine Cicalese, USA, is a former Director of the Joint Command, Control, and Information Operations School at the Joint Forces Staff College.

Report Documentation Page	*Form Approved* *OMB No. 0704-0188*

1. REPORT DATE **2013**	2. REPORT TYPE	3. DATES COVERED **00-00-2013 to 00-00-2013**

4. TITLE AND SUBTITLE **Redefining Information Operations**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University,Joint Force Quarterly ,260 Fifth Avenue, Building 64, Fort Lesley J. McNair,Washington,DC,20319**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**4**	

capability owner, and one that is directed at foreign rather than domestic audiences.

This new IO definition is a long overdue improvement, though one might make the improper interpretation that IO is only about coordinating the themes-and-messages part of the SC "say-do" rubric as it is included within the same overarching DOD memorandum on strategic sommunication. The joint force commander (JFC) should synchronize communication and operation efforts to support the national-level SC process and overall narrative. By conducting IO coordinated with public affairs, the JFC can effectively communicate to the variety of intended audiences and affect adversary decisionmaking to maximize effects in the information environment.

Since 9/11 and the start of the war on terror, the author has frequently heard fellow military officers calling for a supporting global IO campaign. These continuous calls are problematic because, doctrinally, IO in itself is not a campaign. The applicability of a global IO campaign can be challenged as the military cannot apply many IO or information-related capabilities, such as military deception or military information support operations, toward a U.S. domestic audience.

Synchronizing communications and actions may not yet be a doctrinal campaign, but it is vital to support a combatant commander's coherent theater campaign plan. For those who insist on some sort of an information campaign, a synchronized communication plan could supplant the heretofore unending calls for an IO campaign. Because of these reasons and the previous IO core capabilities having improved capacity, one might infer that IO is no longer relevant, as the strategy's narrative or message would be paramount to all information. However, the narrative without IO is not enough to affect decisionmaking.

At the 2011 World Wide IO Conference, much of the first day's discussion supported the notion that strategic communication and IO are the same. The discussion centered on coordinating geographic combatant command Phase 0 (figure 2 depicts the notional phases) messages and the programs that support these activities to shape the operational environment. It was not until the afternoon panel session—when Colonel James Gferrer, then commanding officer of the Marine Corps IO Center, commented, "IO is more than just messaging"[6]—that the conference discussion duly adjusted. IO is much more than coordinating themes and messages or being the military's version of a chattering class.

While several military information-related capabilities deliver a message that can support communication strategy and IO, IO is still about affecting information content and flow as it relates to adversaries' and potential adversaries' decisionmaking cycles. Synchronized communication itself, while a contributing factor, is not enough to affect adversary and potential adversary decisionmaking because it solely focuses on the broadcast or dissemination of the commander's message.

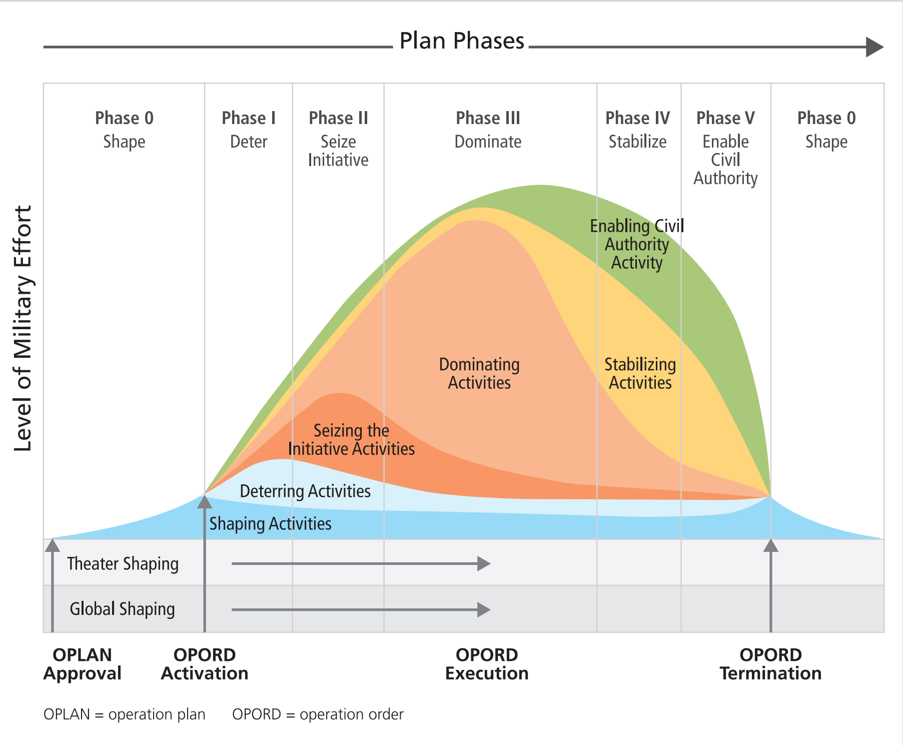
Even though listening, understanding, and assessing are all part of the communication process, the primary communication goal is to send a message. While important, the commander's message is but one of several messages competing for the audience's attention. This only affects the commander's information content output to adversaries and potential adversaries. It does not affect the adversary's information content or flow, neither is it the sole means of protecting the commander's decisionmaking capability. Figure 1 depicts a comprehensive decisionmaking cycle and annotates how the commander's message is part of the dissemination step within this cycle. To affect adversial decisionmaking and protect his own, the commander must demand his IO cell look beyond best practices and templated planning. He must insist upon an agile plan capable of affecting the information environment in more ways than coordinated themes and messages.

More Than Themes and Messages

Just as J2 has the intelligence and counterintelligence mission and J3 (operations) has the fires and counterfires mission, the Information Operations Working Group, on behalf of the commander, should also consider the countermessage mission. Limiting oneself to coordinating and delivering messages as a countermessage mission, however, is insufficient when engaged in a contest as it is both limited and inherently reactive.

Phase 0 (shape) is the predominant phase across the combatant commands, and the commander's communication plan should include all information-related capabilities. Still, the IO professional needs to think beyond just messaging. He needs to maintain a holistic perspective of affecting the adversary's decisionmaking cycle to include part of the countermessage mission.

Figure 2. Notional Operation Plan Phases



OPLAN = operation plan OPORD = operation order

In practice, the IO cell needs to consider a counterinformation or even counterdecision cycle approach.

As former Secretary Robert Gates noted to Congress, "adversaries leverage multiple communications platforms, to proselytize, recruit, fund, exercise [command and control], share tradecraft and perpetuate their ideology. Understanding the increasing complexity of the information environment and the compelling need to leverage information effectively as an element of national power is critical to achieving the Department's military objectives."[7]

Other nation-states have acknowledged a similar approach when they removed media access to their countries' populations. For example, on February 12, 2010, U.S., British, and German broadcasts accused Iran of deliberately jamming their outputs to deny Iranian citizens access to an opinion that counters the Islamic Revolution.[8] Also, on March 12, 2010, Yemeni authorities seized the transmission gear of al Jazeera and al Arabiya channels over their coverage of deadly unrest in the south of the country. Yemeni officials stated such equipment "should not serve to provoke trouble and amplify events in such a way as to harm public order."[9]

Iran and Yemen are not engaged in a legally declared war with one of the offended parties, but they still chose to limit a platform that was disseminating nonsupportive messages. The author does not advocate this tactic as a form of censorship, but instead recognizes the action as part of the IO integrating function. Iran, a potential U.S. adversary, recognizes the value of affecting the information flow of its potential adversaries. IO professionals should understand how to affect the cycle depending on the overall situation more than the designated operational phase. Thus, a geographic combatant commander could ably adjust from Phase 0 to Phase 1 (deter) and future phases depicted in figure 2.

The Wartime Information Cycle

Al Qaeda in Iraq (AQI) demonstrated an understanding of using a range of options to affect information during the period of the organization's apex from February 2006 to July 2007. AQI destroyed antiterrorist radio stations in Baghdad, deliberately assassinated Iraqi reporters in Mosul, and lethally targeted U.S. psychological operations teams in an effort to limit the messaging capabilities of AQI adversaries.

Meanwhile, the coalition inclination to counter AQI information was mostly limited to delivering broadcasted messages via handbill, radio, television, or any standard means of communicating across the tactical, operational, and strategic levels. The proclivity toward using paper resulted in an insufficient "death by a thousand paper cuts" approach.

The tactical coalition commanders saw a threat in AQI's Internet presence. This could have warranted a coalition response to deny AQI freedom of access on the Internet. The Internet presence, however, is just the transmission point within the communication process. An online video of an improvised explosive device destroying a coalition convoy vehicle is the culminating point of the process. A videographer must first record an event and move the video to a point where it can be uploaded to the Internet. Today's videographers often have the means to complete the entire information cycle, thus taking a tactical kinetic attack and transforming it into a strategic information attack.

Presuming the videographer broke host nation law by inciting violence toward legal authorities, the tactical commander could realistically interdict the information cycle by arresting the videographer. The terrorist message is never transmitted—or at least it is delayed—and the ability to keep transmitting is affected without having to fight for authorities to stop a possible Internet transmission. This is how an IO professional must view the situation.

Beyond the Information Cycle

The IO perspective is not limited to counterterrorism or counterinsurgency. It is also applicable in stability or peacekeeping operations (PKO) where adversaries may not be shooting at the U.S. military but are nonetheless in opposition to the combatant commander's objectives and mission. For example, three ethnic groups are vying for position. Two are willing to disarm, but the third and most powerful is reluctant. United Nations (UN) and coalition-led town meetings are popular operations during PKO as a means to bring the belligerent parties closer toward mutual governance. The typical pattern for a town hall meeting is for representatives from the parties to socialize, discuss matters for an hour, come to tentative agreements, and then take a break. During the break, the representatives contact their superiors via mobile devices for further guidance on any tentative agreement. It is not uncommon for one of the parties to return to the meeting with a renewed reluctance to agree with what was otherwise tentatively achieved, such as an agreement to disarm. At this point, the IO professional should consider actions and outcomes to the following possibilities:

- What happens if the town hall representatives are unable to communicate with their superiors during the break and thus unable to renegotiate a new position?
- What happens if a public demonstration calling for immediate disarmament occurs inside or outside the town hall?
- What happens if the host nation media suddenly confront the supreme leader of the most powerful ethnic group over his plans to support a tentative disarmament?

The answers to these questions lie in the IO professional's ability to understand the culture, emotion, and status within the adversary's decision cycle and a way to integrate a variety of activities as a means to inform, influence, or even persuade the adversary into taking action favorable to the commander's mission. While the events may occur around the spoken events of the town hall, the message is but a facilitator to something larger.

To accomplish some of these hypothetical tasks, especially disrupting potential commercial communication means, the IO cell should consult with the electronic warfare and staff judge advocate staff to understand the commander's authorities. According to the UN Charter, electronic warfare jamming may violate national sovereignty and be legally construed as an act of war.[10] Likewise, it may violate the UN General Assembly determination that freedom of information is a human right.[11] Still, these determinations may not apply to the situation. To overcome any limitations, the IO staff must make an argument for what the current situation requires as opposed to what the past allowed. Authorities underpin the mission at all levels, and much of the responsibility for acquiring the authorities for the commander rests on the joint IO staff.

The Authorities Barrier

In spring 2002, the Coalition Forces Land Component Command (CFLCC) in Kuwait developed the ground invasion plan that became known as Running Start. IO planners were embedded within the command's strategic plans and civil military operations teams for planning Phase 2 through Phase 4 (dominance) operations.

The CFLCC commander was keenly interested in the IO plan to support the invasion and wanted a separate brief on it so he could get more details. The attached plans team developed a thorough plan to use the available IO capabilities to support the land component commander mission to destroy Saddam's ground forces by focusing IO efforts to disrupt the decisionmaking of the Iraqi ground forces' center of gravity, the Republican Guard. As a supporting effort, IO would influence the Iraqi people not to interfere with coalition operations. The commander optimized the force and plan to swiftly and violently destroy a nation-state military more than stopping to deliver a message to the Iraqis.

The IO planner was cognizant of a variety of capabilities that could achieve palpable effects to support the CFLCC mission. However, the planner knew of problems in attaining authorities for some of these capabilities. For the prebriefing to J3 leadership, the planner inserted a slide titled "Issues" with five bulleted items to acknowledge up front what the IO plan did not cover. As soon as the J3 saw the slide, he directed the IO planner to remove it from the briefing.

The IO planner was too inexperienced to understand the need never to discuss issues with the commander until the staff tried to resolve them first. While the planner was unable to convince the J3 that the issues were germane to the plan, the intermediate leader was too inexperienced with IO to understand why the issues were significant and assist the staff in resolving them.

When the IO team briefed the CFLCC commander, the commander was dissatisfied with the IO plan. He believed that it did not go far enough and push the envelope. The commander thought IO could win the war without firing a shot. Within the first 5 minutes of the briefing, he inquired about three of the five items listed on the excluded Issues slide. The IO planner was on the right track, but he did not know how to resolve the authority issues.

Later, open source media reports indicated the coalition tried to influence a coup of Saddam from within his inner circle using emails and other means.[12] While no U.S. or coalition government official or agency has ever confirmed this, the notion of instigating a coup that targeted regime member decisionmaking might have satisfied the CFLCC commander's thirst for a more comprehensive IO plan. The planner's lesson learned was to develop a bold yet feasible plan and then seek the authorities to execute the plan instead of accepting the past authorities as an impediment to future plans.

The IO planner later added a second lesson learned. After further analysis, such an attempt to avoid conflict is an example of deterrence. Shape and deter phases matter. Even though Congress is cutting the DOD budget on such information programs,[13] today's joint force continues to invest more time and effort in planning and executing IO throughout the range of military operations.

Conclusion

Joint IO is evolving. The strategic communication process is improving as commanders inform all audiences. IO is much more than coordinating themes and messages. The IO integrator certainly needs to understand the coordinated message but needs to understand the information environment as it relates to the information and decisionmaking cycles of foreign audiences, adversaries, and potential adversaries even more. Communication synchronization is vital, but when the bullets are flying even the best messages are insufficient to affect decisionmaking.

Future military operations will require IO professionals with an understanding of past authority limitations to explore the realm of the possible and justify new operations originating in the information environment. IO, as these vignettes revealed, is never a "cookie-cutter" or "best practices" solution. Planning and executing IO in accordance with its doctrinal definition requires thought and adaptation facilitated by operational analysis.

Meanwhile, many information-related capabilities are growing in capacity. All of this is for the better as the Defense Department's ability to operate within and affect the information environment remains a growth industry. To make the most of these processes and capabilities, the joint force commander needs a limber staff capable of maximizing the commander's options and minimizing staff frictions in order to achieve the commander's effects and complete the mission. **JFQ**

NOTES

[1] "Army establishes Army Cyber Command," available at <www.army.mil/article/46012/army-establishes-army-cyber-command/>.

[2] Curtis Boyd, "The Future of MISO," *Special Warfare* 1 (January–February 2011), 22–29.

[3] Air Force Instruction 10-702, *Operations* (Washington, DC: Headquarters Department of the Air Force, June 7, 2011).

[4] Dennis M. Murphy, "The Future of Influence in Warfare," *Joint Force Quarterly* 64 (1st Quarter 2012), 47–51.

[5] Joint Publication 3-13, *Information Operations* (Washington, DC: The Joint Staff, December 2012).

[6] Colonel James Gferrer approved the author using this quotation from an otherwise nonattribution conference discussion.

[7] "Request for Support of Funding Authorities to Combat Information Operations," Office of the Secretary of Defense, Washington, DC, 2010.

[8] "International Broadcasters Condemn Iran Over 'Jamming,'" BBC, available at <http://news.bbc.co.uk/2/hi/8511921.stm>.

[9] "Yemen Seizes Arab Satellite TV Gear Over Southern Unrest," Agence France-Presse, available at <www.google.com/hostednews/afp/article/ALeqM5gkrWanPN6xBGeMX_ax8TdFNrC9Ow>.

[10] United Nations, Charter of the United Nations, 7/51, October 24, 1945, available at <www.un.org/en/documents/charter/chapter7.shtml>.

[11] GA Res 424 (V), UN GAOR, 5th Sess., Supp. No. 20, UN Doc. A/1775 (1950), ("Freedom of information is a human right.").

[12] Peter Ford, "Is it too late for a popular uprising inside Iraq? Refugees report signs of unrest in Baghdad," *Christian Science Monitor*, January 27, 2003, 14.

[13] Walter Pincus, "Lawmakers Slash Budget for Defense Department's Information Ops," *The Washington Post*, June 22, 2011, available at <www.washingtonpost.com/blogs/checkpoint-washington/post/lawmakers-slash-budget-for-militarys-information-ops/2011/06/22/AGVC3cfH_blog.html>.