Soldier with 780th Military Intelligence Brigade sets up cyber tools overlooking mock city of Razish at National Training Center, Fort Irwin, California, May 5, 2017, as part of Army Cyber Command–led Cyber-Electromagnetic Activities Support to Corps and Below Initiative (U.S. Army Cyber Command/Bill Roche)

The Practical Implications of Information as a Joint Function

By Gregory C. Radabaugh

The importance of understanding the informational aspect of the operating environment was underscored by the Chairman of the Joint Chiefs of Staff's addition of Information as a Joint Function (IJF) in a recent change to Joint Publication 1, *Doctrine for the Armed Forces of the United States*. This change comes amid an erosion of the U.S. military's competitive advantage in a security environment marked by challenges from Russia, China, Iran, North Korea, and violent extremist organizations (VEOs). As the Chairman articulated in his 2016 posture statement, conflict with one—or a combination—of our adversaries will be transregional, multidomain, and multifunctional (TMM) in nature. This represents a marked shift from how past conflicts were fought and will put significant stress on the Department of Defense's (DOD's) geographically based operational structure and associated command and control (C2) architecture. Future conflicts "will spread quickly across multiple combatant command geographic boundaries, functions, and domains. We must anticipate the need to respond to simultaneous challenges in the ground, air, space, cyberspace, and maritime domains."[1]

Among the many challenges affecting operations in and across all the domains are advances in information technology, which have significantly changed the

Gregory C. Radabaugh is Director of the Joint Information Operations Warfare Center, Joint Base San Antonio, Texas.

Soldier with Expeditionary Cyber Electromagnetic Activities Team, 781st Military Intelligence Battalion, conducts cyberspace operations at National Training Center, Fort Irwin, California, May 9, 2018 (U.S. Army Cyber Command/Bill Roche)

generation, transmission, reception of, and reaction to information. As highlighted in the *Joint Concept for Operating in the Information Environment*, "these advances have increased the speed and range of information, diffused power over information, and shifted sociocultural norms. The interplay between these three provides our competitors and adversaries additional opportunities to offset the diminishing physical overmatch of the world's preeminent warfighting force."[2]

This three-way interplay affects each of the warfighting domains and their activities in the information environment (IE). For example, operations in the land domain will increasingly take place among, against (in the case of VEOs), and in defense of civilians. Civilians will be the information targets and the objectives to be won, as much as an opposing force.[3] Similarly, since deterring conflict also hinges ultimately on perceptions and attitudes, the joint force will require an understanding of how relevant actors perceive and understand information. In all domains, every friendly action, written or spoken word, and displayed or relayed image has informational aspects that communicate a message or intent.[4] Commanders must also be alert that red actors will interpret blue activities through the lens of their personal world views, regardless of the intended message.

With IJF, commanders must now understand the centrality of dynamic integration of information with other joint functions (C2, fires, intelligence, movement and maneuver, protection, sustainment) in order to positively alter relevant actor perceptions and behaviors in a TMM security environment regarding national security objectives.

Command and Control. Information is integral to planning for and synchronizing operations involving disparate entities (and their associated capabilities and processes); all require a collective understanding of the implications and character of the warfighting domains and IE. The Services are pursuing new ways of thinking and training and new technologies to collect and distribute data for situational awareness coupled with real-time reporting of the changing battlespace.[5] Mission command in the IE, for example, entails commanders giving subordinates the flexibility to adjust a theme, narrative, and message as the situation dictates.

Fires. Commanders will be more likely to consider the employment of *all* available weapons and other systems. The Marine Corps has recently established an Information Marine Expeditionary Force to build and sustain effective offensive cyber and electronic warfare operations and associated intelligence support. Fires and information also extend to the synchronization of information-related activities such as military information support operations with hard assets like a GBU-43/B Massive Ordnance Air Blast (the so-called Mother of All Bombs) to blunt adversary uses of ideas, images, and violence designed to manipulate the United States and its allies.

Intelligence. Commanders can be expected to place increasing emphasis on the integration of intelligence disciplines and analytic methods to characterize, forecast, and assess the IE. Moreover, they will be more inclined to emphasize it early in the planning process due to the long lead time needed to establish information baseline characterizations and properly assess effects in the IE. A major challenge will be characterizing the informational battlespace in a way that enables commanders to visualize it in the same manner as the land, sea, air, space, and cyberspace battlespaces, enabling them to fully integrate informational and physical power.

Movement and Maneuver. This function includes moving or deploying forces into an operational area and maneuvering to achieve objectives. In developing plans ranging from freedom of navigation to those intended to prevent a crisis from worsening and allow for de-escalation (flexible deterrent options), IJF will provide a means for commanders to more tightly align the movement of forces with information activities to influence relevant actors. Every physical activity has an informational component.

Protection. The protection function in part includes conserving the joint force's fighting potential by making friendly forces difficult to locate and strike. Integration of protection and information—particularly regarding military deception and operations security (OPSEC)—will be critical to antiaccess/area-denial operations, where the joint force will have to maneuver undetected over strategic distances through multiple domains.

Sustainment. Sustainment is the provision of logistics and personnel services necessary to extend operational reach. Management of information and information systems is critical to sustainment and will be a significant target of adversary attack. Thus, commanders must integrate OPSEC into sustainment planning as they do in planning other aspects of operations.

In addition to enhancing joint warfighting today, IJF in joint doctrine will play a significant role in three ways. First, while policy generally drives doctrine, on occasion a new application of an extant capability within doctrine may require the creation of policy. In the coming months, senior-level forums (for example, the Information Operations Executive Steering Group) comprised of policymakers, operators, and doctrine developers can be expected to work collaboratively to develop effective and integrated policy and doctrine for the joint force.

Second, joint doctrine provides the foundation for joint training and education. As such, curricula from precommissioning programs to general and flag officers continuing education programs will be revised to reflect the informational aspects of all military activities.

Finally, while not the explicit goal of IJF, its incorporation into joint doctrine opens the possibility for changing the way DOD programs and budgets for operations in the IE. Joint functions are generally aligned with Joint Capability Areas (JCA), which are collections of like-capabilities functionally grouped to support capability analysis and investment decisionmaking. JCAs are aligned with Functional Capability Boards, which assist the Chairman in accomplishing his statutory responsibilities of assessing risk and making programmatic recommendations. Now that information is a joint function, changes within the Planning, Programming, and Budgeting Execution process could follow, making needed investments for operations in the IE more visible (such as creating a separate Information JCA).

The integration of the IJF with the other six joint functions offers new opportunities for developing and conducting operational art and design. IJF will result in the development of executable plans to deal with future conflicts that are TMM in nature. Moreover, given the importance of joint doctrine to other foundational aspects of combat power and the way in which DOD accomplishes programming and budgeting actions, IJF will serve to create a joint force of tomorrow more capable of and organized to leverage the inherent informational aspects of all military activities to achieve the commander's objectives and enduring strategic outcomes. The ultimate result will be that joint force commanders are able to dominate the informational aspect of their operating environment (the IE) the same way they dominate land, sea, air space, and cyberspace. **JFQ**

Notes

[1] Posture Statement of General Joseph F. Dunford, Jr., before the Senate Armed Services Committee, March 17, 2016.

[2] *Joint Concept for Operating in the Information Environment* (Washington, DC: The Joint Staff, September 1, 2017, draft version 0.80).

[3] General Sir Rupert Smith described this construct as "war amongst the people." See Rupert Smith and Ilana Bet-El, "Military Capabilities for War Amongst the People," in *Adapting America's Security Paradigm and Security Agenda*, ed. Roy Godson et al. (Washington, DC: National Strategy Information Center, 2011).

[4] Joint Publication 1, *Doctrine for the Armed Forces of the United States* (Washington, DC: The Joint Staff, March 25, 2013).

[5] David L. Goldstein, *Enhancing Multi-Domain Command and Control . . . Tying It All Together*, U.S. Air Force Focus Area (Washington, DC: Headquarters Department of the Air Force, 2017); and Mark A. Milley, *Multi-Domain Battle: Combined Arms for the 21st Century* (Washington, DC: Headquarters Department of the Army, February 2017).