Information Operations:
Doctrine, Tactics, Techniques and Procedures©

Lieutenant Colonel Richard H. Wright, US Army, Retired

BEFORE Operation *Desert Storm*, information-based doctrine was known as command, control and communications countermeasures (C^{3}CM). As discussed in Joint Publication (JP) 3-13, *C^{3}CM in Joint Operations*, the four components of C^{3}CM are jamming, destruction, deception and operations security (OPSEC).[1]

> **Joint doctrine arbitrarily places each element under either offensive or defensive IO. The Army believes this approach to is too restrictive and that the elements are equally applicable to either offensive or defensive operations.**

Desert Storm showed a need for the same command, control and communications (C^3) capability regarding tactical weapons. Paper maps and grease pencils were still essential to data exchange. The physical-destruction mission against enemy command and control (C^2) facilities, supported by OPSEC, military deception, psychological operations (PSYOP) and electronic warfare (EW), prevented effective employment of enemy forces. Despite the shortcomings between maneuver and C^3, *Desert Storm* became a prototype for information-based warfare.[2]

In 1992 a series of Department of Defense (DOD) documents were written on information operations (IO). Beginning in 1994, the US Army Training and Doctrine Command (TRADOC) published a series of publications that included information-based processes relating to C^2:

- TRADOC Pamphlet 525-200-5, *Depth and Simultaneous Attack*.[3]
- TRADOC Pamphlet 525-5, *Force XXI Operations*.[4]
- US Army Field Manual (FM) 100-6, *Information Operations*.[5]

In early 1996, DOD and joint documents were published using the term "information warfare" with "command and control warfare" (C^{2}W) as a subset. The Army determined the term "information operations" was more descriptive because land forces were involved in offensive and defensive combat operations as well as support and stability operations.

In late summer 1996, after TRADOC Deputy Chief of Staff for Doctrine published FM 100-6, the next version was passed to the Combined Arms Doctrine Directorate (CADD), US Army Command and General Staff College, Fort Leavenworth, Kansas. Since then several brigade, division and corps warfighting experiments have been conducted. These, as well as operations in Bosnia and Kosovo, validated IO as an increasingly important element of combat power.

Why the Army Needs FM 3-13

The Army needs this manual to understand how IO helps accomplish missions. The Doctrine Review and Approval Group (DRAG) version of the new FM 3-0, *Operations,* formally identifies information as an element of combat power.[6] By gaining information superiority, commanders gain a decisive information advantage over the adversary. Interactive and pervasive IO occurs within the information environment and contributes to achieving information superiority. IO is not new, but the synergistic effect created by using its elements either offensively or defensively is new. The interaction of offensive and defensive IO leads to information superiority which, in turn, allows commanders to seize, retain and exploit the initiative during operations.

Today the digitized systems in corps and divisions allow commanders to reach beyond the days of *Desert Storm*. FM 3-13, *Information Operations: Doctrine, Tactics, Techniques and Procedures*, operationalizes IO doctrine and makes it useful to units planning and executing IO under these modernized conditions.

Differences Between the 1996 and 2000 Manuals

The Army led the joint community in IO when it published FM 100-6 in 1996. The authors did an outstanding job of bringing IO into the Army lexicon and causing leaders to think about and debate the role of IO in mission planning. The manual's framework was built around three interlocking areas: operations (including of the elements of C^{2}W—OPSEC, military deception, EW, destruction and PSYOP—public affairs [PA] and civil affairs [CA]); relevant information and intelligence (RII); and information systems (INFOSYS).[7] While the doctrine was well-conceived and well-written, it was heavy on theory and light on practice, and the definitions tended to be long and repetitive. Units encountered numerous difficulties in operationalizing IO tenets. What the field wanted was practical tactics, techniques and procedures (TTP) to bridge this gap.

Seven months before the publication of FM 100-6, JP 3-13.1, *Joint Doctrine for Command and Control Warfare (C^{2}W)*, was published. However, by addressing only C^{2}W, it did not meet the Army's requirements for IO TTP. In particular, the publication did not address PA and CA.

A new version of JP 3-13, *Joint Doctrine for Information Operations*, was released in 1998. The publication excluded C^{2}W and introduced IO as an overarching concept consisting of offensive and defensive IO. It also introduced PA and CA as related activities and not integral elements of IO, as did FM 100-6.[8] This change put the Army's 1996 IO doctrine out of step with the 1998 joint IO doctrine. In addition to the five original IO elements, JP 3-13 added counterpropaganda, counterdeception, computer network attack, information assurance, physical security, counterintelligence and special IO elements.[9] Offensive and defensive IO replaced C^2W as the term for using these elements. This new JP was a major step toward meeting the Army's IO needs.

During the transition of IO doctrine from 1996 through 2000, CADD discovered the previous paradigm of operations, RII and INFOSYS, did not fit neatly into formulating a revamped Army IO doctrine. Additionally, during the Battle Command Training Program (BCTP) Warfighters and Division Advanced Experiments, corps and division staffs did not discuss IO in relation to how to attack the enemy or defend friendly C^2 but, rather, how to use IO in the tactical operations centers. As a result, INFOSYS and RII were separated and placed in FM 6-0, *Command and Control*, as information management (IM). IM directly relates to assisting the commander in C^2.

Joint and Army definitions differ because the Army recognized that information superiority's only value is its operational advantage over the enemy. FM 3-0 also discusses how information superiority supports full-spectrum operations, to include offense, defense, and stability and support operations.

This left IO consisting of the elements described. Initially, proposals for updating FM 100-6 were modest, simply updating the 1996 version with changes in joint doctrine and proposing a second manual, FM 100-6-1, for TTP. However, preparatory work with the BCTP, Land Information Warfare Activity (LIWA) and Center for Army Lessons Learned (CALL) demonstrated that FM 100-6 needed a major rewrite to capture IO doctrine and TTP.

The new manual combines LIWA lessons learned in Bosnia and BCTP corps and division warfighters. Including TTP in the 2000 manual is the most significant change between the 1996 and 2000 manuals, a direct result of input from corps and division staffs, observations during Warfighters, and the real-world experiences of members of LIWA's field support teams in Bosnia and Kosovo.

At the same time the 2000 version was drafted, work on FM 3-0, *Operations*, was under way.[10] In FM 3-0, information superiority is discussed in detail, as is the framework for IO and IM. As a result of the FM 3-0 work, intelligence as the underpinning of IO was changed to intelligence, surveillance and reconnaissance.[11]

The Difference Between Army and Joint IO Doctrine

Army IO doctrine gets its lead from joint IO doctrine but modifies the content to fit Army needs. JP 3-13 defines information superiority as "the capability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[12] FM 3-0 defines information superiority as "the operational advantage delivered from the ability to collect, process and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same." Joint and Army definitions differ because the Army recognized that information superiority's only value is its operational advantage over the enemy. FM 3-0 also discusses how information superiority supports full-spectrum operations, to include offense, defense, and stability and support operations.[13] FM 3-13 continues this discussion of IO as it contributes to achieving information superiority. FM 3-0 and FM 3-13 define IO as the actions that target adversaries' info systems, "and influence others' decision-making processes, information and information systems while protecting one's own information and information systems."[14] JP 3-13 defines IO as "action taken to affect adversary information and information systems while defending one's own information and information systems."[15] The joint definition does not recognize that land forces routinely encounter entities other than friendly forces and enemy forces on the battlefield. These "others" represent a diverse group of actors, such as nongovernment organizations, refugees and neutral governments, each of which may significantly impact a commander's plan if their motives, needs and presence are not recognized and addressed.

Another departure from joint IO doctrine is in defining and applying offensive and defensive IO. The IO elements were restricted to five under the C^2W construct; later joint doctrine expanded the number to 13. Joint doctrine arbitrarily places each element under either offensive or defensive IO. The Army believes this approach to is too restrictive and that the elements are equally applicable to either offensive or defensive operations. The Army's definition of offensive and defensive IO further reflects this philosophy. The Army's definition of offensive IO is "the integrated use of assigned and supporting capabilities and activities, mutually supported by intelligence, to affect enemy decision makers or to influence others to achieve or promote specific objectives."[16] Its defensive IO definition is "integration and coordination of policies and procedures, operations, personnel and technology to protect and defend friendly information and information systems. Defensive IO ensures timely, accurate and relevant information access while denying adversaries the opportunity to exploit friendly information and information systems for their own purposes."[17]

A third difference is in information systems. The Army's definition of information systems is "the equipment and facilities that collect, process, store, display and disseminate information. This includes computers, hardware and software, communications, and policies and procedures for their use."[18] The joint definition is broader: "the entire infrastructure, organization, personnel and components that collect, process, store, transmit, display, disseminate and act on information."[19] FM 6-0 describes the reason for the difference, but essentially, the joint definition places commanders *in* the information systems.

Army IO doctrine does not differ from joint IO doctrine regarding PA and CA. Both agree they are related activities and have larger missions. The Army does operationalize CA in terms of civil-military operations.

Today's challenge is training corps and division headquarters. For commanders to be confident in their IO programs, they must witness IO's true synergistic power at all levels.

The Value of Info Ops

The US Army has, in the past, used the individual IO elements with great effect. Over the past several years, the Army has recognized that IO can only reach its true potential when its subordinate elements are employed in a concerted, coordinated fashion. IO's true added value comes from collective, synergistic employment. Bringing the planning and execution together under one staff officer ensures that the major positive aspects of each are executed and the negative aspects of each are deconflicted.

Today's challenge is training corps and division headquarters. For commanders to be confident in their IO programs, they must witness IO's true synergistic power at all levels. This responsibility falls to the IO coordinator, a coordinating staff officer working directly for the chief of staff. This new coordinating staff officer position shows that IO cuts across all staffs and needs central planning and deconfliction of individual elements. The intent is not to take IO responsibility away from other coordinating staffs but to reinforce this responsibility. Every staff member plays a vital role in achieving information superiority in accordance with the commander's intent.

It was with this goal in mind that FM 3-13 was written. Giving the staff detailed TTP and a coherent doctrinal structure for its employment condenses principles and procedures into a unified process. The staff will gain a common starting point from which to apply doctrine to local conditions and missions.

TTP focus on operationalizing IO support of the military decision-making process (MDMP). They provide specific connectivity between IO and each step of the MDMP, addressing major criticisms of the 1996 manual — that IO was not well integrated in ongoing staff processes and procedures. Preparing and executing IO complete the TTP. This part of the manual will be the greatest help to staff officers new to IO.

The manual contains a number of appendixes that cover specific aspects of IO:

- IO actions and outputs during each step of the MDMP.
- An IO staff estimate format.
- An annotated IO annex format. In the 1996 manual, the example was a C^2W annex.
- IO input to the targeting process; some IO cell outputs are inputs to the targeting process.
- An IO scenario with example inputs, actions, activities and forms shows IO's importance to an operation.
- IO duties of coordination and special staffs—the basis upon which combat developers can create an IO section at corps and division levels.
- OPSEC doctrine to supplement the regulation.
- Doctrinal update on deception tied to MDMP.
- The role and responsibilities of LIWA.

Information operations are not new to the Army, but in many ways, the Army is new to information operations. As the world enters the information age, the US Army must be prepared to fight adversaries with every advantage technology provides. Likewise, to succeed, it must defend its own information systems and processes from disruption or destruction. FM 3-13 provides the doctrinal basis for this transition.

NOTES

[1] MAJ Arthur N. Tulak, Master of Military Arts and Science Thesis, *The Application of Information Operations Doctrine in Support of Peace Operations* (Fort Leavenworth, KS: US Army Command and General Staff College, 1999), 16.

[2] Ibid., 17.

[3] Ibid., 19.

[4] Ibid.

[5] Ibid.

[6] US Army Field Manual (FM) 3-0, *Operations* (Washington, DC: US Government Printing Office [GPO], 11 August 2000), 4-10.

[7] FM 100-6, *Information Operations* (Washington, DC: GPO, 27 August 1996), 2-3.

[8] Chairman of the Joint Chiefs of Staff, Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations* (Washington, DC: GPO, 9 October 1998), 1-9.

[9] Ibid.

[10] While the manual was being written, TRADOC introduced a new numbering system to parallel that of joint manuals. Thus, FM 100-5, *Operations*, was changed to FM 3-0, and FM 100-6 was changed to FM 3-13 to correspond to JP 3-13.

[11] FM 3-0, 11-6.

[12] JP 3-13, 1-10.

[13] Ibid., 11-2.

[14] FM 3-0, 11-17.

[15] JP 3-13.

[16] FM 3-0, 11-17.

[17] Ibid.

[18] Ibid., 11-11.

[19] JP 3-13, I-11.

Lieutenant Colonel Richard H. Wright, US Army, Retired, is a military analyst and author of US Army Field Manual 3-13, Combined Arms Doctrine Directorate, US Army Command and General Staff College, Fort Leavenworth, Kansas. He received a B.A. from North Georgia College and an M.A. from the University of Southern California. He is a graduate of the US Army Command and General Staff College. He has served in various command and staff positions in the Continental United States and Germany, including Junior ROTC instructor, St. Joseph, Missouri; analyst, Department of Tactics, US Army Command and General Staff College, Fort Leavenworth; and S3 and installation coordinator, 210th Field Artillery Group, Herzo, Germany.