SMALL WARS JOURNAL

smallwarsjournal.com

To Kill a Mockingbird: The Deconstruction of Information Operations

Randolph Rosin

With the publishing of FM 3-0 in February 2008, the Army ushered in a new information doctrine. Based on the premise of an operational environment of increasing informational complexity, the Army made the determination that the current concept of information operations (IO) was too limiting in scope and necessitated a paradigm shift.[1] The problem set, as defined by the Combined Arms Center (CAC), was "an inadequate capability to communicate effectively and coherently;" "no single cyber/cyberspace theory;" and "a perception that IO has somehow failed to deliver the goods."[2]

To address this problem set, CAC created a conceptual framework based on five information tasks consisting of information engagement (IE), Command and Control Warfare (C2W), information protection, Operations Security (OPSEC) and military deception (MILDEC). IE is intended to address the first problem of an inadequate capability to communicate effectively and coherently while C2W and information protection intend to address the cyber/cyberspace issue. Organized along functional lines, former IO capabilities disaggregate and reapportion to different staff sections. Consisting of a blend of public affairs, Functional Area (FA) 30 and PSYOP personnel, IE is the staff responsibility of the G7. Electronic warfare (EW) and computer network operations (CNO) form the C2W cell under the fires support coordinator (FSCOORD). Information protection, formerly information assurance, remains with the G6; OPSEC belongs to G3 Protect, and MILDEC, to G3 plans. Effectively, the new Army doctrine deconstructs the IO concept.

In deconstructing IO, the Army is pursuing an independent path that diverges significantly from the rest of the Department of Defense (DoD) and, in so doing, begs the question whether or not it is heading down the right path. Because the information domain cuts across traditional military distinctions of land, air and sea domains, a common joint understanding of concepts becomes an imperative to ensure unity of effort. In pursuing an independent path from DoD Directives and joint doctrine, legitimate questions arise as to whether this contributes to joint interoperability and unity of effort, as well as whether this supports the Army's Campaign Plan with respect to fielding a "joint and expeditionary Army with campaign capabilities." Moreover, a critical eye should be applied to the emerging doctrine with respect to whether or not it will actually deliver greater capability to the commander. This paper contends that the new doctrine emerges from

[1] Combined Arms Center, "FM3-13 Information Brief to CSA," briefing slides, Fort Leavenworth, KS, 27 February 2009.

[2] Ibid.

flawed premises, offers less capability to the commander, and does not support the Army's Campaign Plan.

Genesis of the New Doctrine

To understand the genesis and logic of the new Army doctrine it is instructional to note the writings of Brigadier General (BG) (ret) Huba Wass de Czege. CAC engaged BG (ret) Wass de Czege as a consultant and his writings are directly reflected in FM 3-0 Operations and the new FM 3-13 Information. In a series of articles published on the Small Wars Journal blog site and in the Military Review, he provides key insights into the genesis and logic behind the doctrine. Wass de Czege reveals that then LTG Petraeus, as the CAC Commander and IO proponent Chief, asked him to "take a fresh look at IO."[3] In pursuing his study, he relied on reviewing doctrinal literature, professional journals, conference reports, interviews and units in training.[4] Wass de Czege approached his study with several questions in mind, among the more prominent were: "How can we better achieve information superiority and enhanced effects?" "What is the best way to integrate the core capabilities...in concert with supported and related capabilities to influence, disrupt, corrupt or usurp adversarial human and automated decision-making, while protecting our own?" "What are the best practices in the field?"[5] Other questions he considered were, "are we getting the most 'Value Added' from IO core, supporting, and related capabilities that we could?;" "how has the nature of the problem changed since the 1990s?" and "what do commanders need IO capabilities to do for them?"[6] To be sure, these questions posed valid points of departure for his study.

Wass de Czege concluded from his study that IO doctrine was untenable and nothing short of a complete overhaul of Army information doctrine would enable it to face the challenges in current and future operating environments. According to Wass de Czege, the reasons why it is necessary to undertake a radical restructuring are that current IO doctrine "misframes" the problems since 9/11; U.S. forces gain less from these capabilities and competencies than it might otherwise be capable of; the notion of a separate logical line of operation for IO inhibits the integration of IO capabilities with multiple objectives; and, that a single staff officer could not effectively employ IO capabilities.[7] With regards to "misframing," Wass de Czege asserts that IO doctrine, having been initially developed in the 1990s, is best suited against a "modern, well-defended rogue regime that we see as a mirror image of ourselves" and does not adequately address contemporary problem sets.[8] Deriving greater benefit from the IO capabilities is tied to the idea that a single staff officer cannot effectively employ the capabilities and that they should align under the appropriate staff section for oversight according to "common functional purposes, causal logic, and art and science based competencies."[9] Additionally, Wass de Czege maintains that it is more important to link actions and deeds than the integrated employment of IO capabilities. Finally, based on the complexity of today's operating environment, Wass de Czege

[3] Huba Wass de Czege BG (ret),"Rethinking "IO:" Complex Operations in the Information Age," July 4, 2008, http://smallwarsjournal.com/mag/2008/07/rethinking-io-complex-operatio.php (accessed September 10, 2008)
[4] Ibid.
[5] Ibid.
[6] Ibid.
[7] Ibid.
[8] Ibid 3
[9] Ibid.

recognizes the necessity to simultaneously pursue multiple objectives and contends that having a separate logical line of operation (LLO) for IO prevents the application of IO capabilities in support of other objectives. These conclusions, that Wass de Czege reached, form the foundation on which the new doctrine stands.

An Examination of the Premises

Given that his conclusions form the basis of the new information doctrine, it is necessary to examine the manner in which he arrived at them. In terms of how Wass de Czege structures his argument, there are flaws regarding his logic and the means by which he arrives at his conclusions. His flaws in logic are the *non sequiturs* and false analogies he employs, as well as analytic propositions that are derived primarily through *a priori* knowledge. Throughout his writings there is a notable lack of empirical and experiential knowledge demonstrated in support of his propositions. With respect to *non sequiturs*, Wass de Czege attempts to make his case against the IO construct by representing the inadequacy of current command processes to meet the challenges of today's complex missions as being flaws in the IO paradigm. Specifically, Wass de Czege stresses the importance of the coherence of words and deeds and derides the notion of a separate IO LLO and represents this as being a matter of IO doctrine. In fact, these elements are a part of the operational framework established by the commander and his staff and not inherent to IO. By definition, LLOs assist the commander and staff to, "visualize and describe the major efforts/actions of the campaign."[10] As well, if there is not coherence in words and deeds, it is a matter of how the commander visualized the operation, framed the problem and articulated his concept. Ironically, in a follow-on article on unifying physical and psychological effects, Wass de Czege makes the case that commanders and operation officers should, "as second nature," be aware of the blending of the psychological and physical dimensions of operations.[11] The real issue is not with the IO paradigm, but with how commanders and staffs approach operational design in complex and irregular environments, which is a matter of their training and education.

Another significant flaw in his argument is the proposition that the IO paradigm "misframes" the problems currently facing IO operators and unit commanders. His contention that because IO is a 1990s construct designed specifically to be used against modern rogue states in our mirror image and thus not suitable for current and future environments misrepresents what IO is relative to. The IO paradigm is not tied to a specific adversary such as Air Land Battle doctrine was to the Soviets, but is relative to the ways and means humans use to communicate and their cognitive processes. If our adversaries watch television, listen to radios, read newspapers, use hand-held devices, operate computers and depend on the backbone of wireless technology, broadband, and satellite connectivity, the IO paradigm remains an eminently valid concept. The problems facing IO operators and unit commanders are not a matter of "misframing" a paradigm but in training, education, resources and authorities.[12]

[10] Jack Kem, *Campaign Planning: Tools of the Trade* (Ft Leavenworth, KS: U.S. Army Command and General Staff College), 111.

[11] Huba Wass de Czege BG (ret), "Unifying physical and Psychological Impact During Operations," *Military Review*, no. 2 (March-April 2009): 14.

[12] Major Joseph Cox provides a thorough analysis on IO shortcomings with respect to doctrine, intelligence, resourcing, training and education in his monograph, Information Operations in Operations Enduring Freedom and Iraqi Freedom (Fort Leavenworth, KS: U.S. Army Command and General Staff College, 2006)

From an empirical standpoint, Wass de Czege's propositions are not well supported. Wass de Czege states that he based his study on his review of doctrinal literature, professional journals, conference reports, interviews of recently deployed IO veterans, and visits to units in training.[13] Clearly, the primary basis of his study is anecdotal evidence and not rigorous data collection and analysis. There is no indication, on his part, of a comprehensive and broad data collection from IO operators actually "in contact" in theaters of war. Had he done so, in all likelihood, he would have reached different conclusions. Indeed, the Center for Army Lessons Learned (CALL) in conjunction with the Army Capabilities Integration Center (ARCIC), conducted such a comprehensive report, in which none of the observations, insights, and lessons learned support Wass de Czege's prognosis and subsequent prescriptions for change.[14] The IO portion of III Corp's after action report (AAR) as the Multi-National Corps- Iraq (MNC-I) headquarters, also does not indicate support for Wass de Czege's conclusions.[15] As well, a survey of all the CALL publications related to IO reveals little to support Wass de Czege propositions.

Mostly though, Wass de Czege's argument for drastic change is weak because his analytical propositions depend on rational deductions that have serious problems when exposed to experiential based knowledge. Experientially, most of his propositions do not reflect current practices. Highlighting the current practices at MNC-I, which has six years of experience conducting operational IO and is the largest sustained IO program executed by the U.S. military, is illustrative. For one, it is not common practice for plans to have a separate IO LLO. The last four operational plans developed by MNC-I spanning 2006-2009, did not contain a separate IO LLO as the lines of effort integrate IO[16]. With respect to the coherence of words and deeds, commanders have grasped the concept that one must create "facts on the ground" that an IO plan leverages to amplify effects. Failing to improve security, while extolling how good security is, is counterproductive and damages the credibility of the command. As well, there is wide recognition that there is value to an action whose primary purpose is to produce a psychological effect and the importance of accompanying messaging to frame the action and enhance the overall impact. It is important to note, once more, that this is not a function of IO but how a commander visualizes his operations and how his staff develops the operational framework.

An Examination of the Information Organizational Construct

Most tellingly, Wass de Czege's prescriptions for change as articulated in FM 3-0, DA Pam 600-3 and the draft FM 3-13, are not practiced in reality. In the Iraq Theater of Operations (ITO), no Army units organize or operate according to the new doctrine. Because the new doctrine does not provide commanders with a realistic or effective construct, units organize and operate in a multitude of ways. Currently, Multinational Divisions (MNDs) are organized and operate according to a hybrid of joint IO doctrine, new Army information doctrine, and old FM 3-13 doctrine. There is not a unit in Iraq that fully embraces the new doctrine. This is so, not because

[13] Wass de Czege, *Rethinking "IO:" Complex Operations in the Information Age*.
[14] Center for Army Lessons Learned, *Gap Analysis Information Operations*, No.08-31 (Ft. Leavenworth, KS: Combined Arms Center, May 2008).
[15] Center for Army Lessons Learned, *III Corps as MNC-I Initial Impressions Report*, (Ft. Leavenworth, KS: Combined Arms Center, August 26, 2008).
[16] MNC-I OPLANS 08-01, 08-02, 09-01, 09-02.

commanders are the “illiterate of the 21st century” lacking the ability to “learn, unlearn, and relearn,” as Wass de Czege infers, but because, faced with the exigency of producing actual effects, commanders recognize that integrated IO capabilities provide them with the maximum benefit from those capabilities and are hesitant to commit to an unproven concept .[17] In spite of Wass de Czege’s contention that commanders would gain more from IO capabilities apportioned to various staff sections, it is obvious that the field rejects this theoretical proposition, and chooses to sustain a construct that, in reality, delivers the desired effects.

At this point, it is necessary to examine Wass de Czege’s proposition, resident in the new information doctrine, that commanders would achieve maximum benefit from IO capabilities when dispersed among different staff sections. Wass de Czege bases his proposition on the idea that the output of IO core, supporting and related capabilities need to be integrated with multiple lines of operation rather than integrated under the current IO construct in a separate LOO.[18] Based on this logic, he proposes that the capabilities be broken out of the IO construct and placed under the staff sections that contain like functions. According to his rationale, electronic warfare and computer network attack are considered to be weapon systems because “they can be aimed at targets” like artillery and can suppress the functioning of equipment and networks and therefore belong under the staff supervision of the FSCOORD.[19] MILDEC, because it’s a planning function, belongs in the G-5 and staff oversight of OPSEC, a command responsibility, belongs to the G3 and is resident in the Protect Branch.[20] While noting the IO proponent advocated for the G7, a Functional Area (FA) 30 IO officer position, be the cross-functional integrator of PA and PSYOP, Wass de Czege supports this construct as it fulfills his sense of the need to have a military public relations function.[21] The purpose of the military public relations function, or what in doctrine is being called information engagement (IE), is to speak for the command to all foreign and domestic audiences.[22] In light of this “military relations function,” he would restrict application of PSYOP to hostile opponents and limit its function to “clarifying and amplifying” for those opponents the “implied message of the unit’s mission and actions.”[23] Because PSYOP would only be directed at opponents, it would be excluded from being used to provide public information to foreign populations to support humanitarian activities, restore civil order, and civil-military operations.[24] According to Wass de Czege, this distribution of IO capabilities is supposed to provide commanders with greater value from those capabilities and allow them to operate more effectively in contemporary and future operating environments than the legacy IO paradigm. However, because Wass de Czege arrives at this proposition largely through rational deduction, it remains an unproven concept, untested by actual operational experience.

In view of actual experience and practice, it is instructional to compare how a legacy IO construct addresses a given problem-set and contrast it with the new paradigm. In a planning

[17] Wass de Czege.
[18] Ibid.
[19] Ibid.
[20] Ibid.
[21] Ibid.
[22] Ibid.
[23] Ibid.
[24] U.S. Department of the Army, *Commissioned Officer Professional Development and Career Management,* Pamphlet 600-3 (Washington, DC: U.S. Department of the Army, 11 December 2007), 172.

scenario, the IO coordinator in a legacy IO organization directs the OPSEC planner to conduct a vulnerability analysis on a plan in development and to craft a mitigation strategy that includes a MILDEC requirement. The OPSEC planner identifies the requirement and passes it to the MILDEC planner, who then develops the overall CONOP. Because he sits in the same cell, he directly engages the PSYOP officer for assistance in developing the culturally specific messages and possibly some of the means to reach the target audience (TA). Depending on the TA and the desired effect, the means to reach the TA might be through technical applications, space assets and/or CNO. Because the IO coordinator has these capabilities and the requisite subject matter experts resident in his staff section and FA 30s who possess the core competencies and experience to plan the integration of these capabilities, he is able to guide the development of the CONOP through the process and its execution. As well, when supervising the development and execution of the plan, the IO coordinator can apply more resources if need be to support execution of this CONOP. Bringing together IO capabilities to produce effects under this scenario is a straight-forward prospect.

In contrast, under the new information doctrine, this same scenario would prove more difficult in addressing the problem-set. First, the G3 Protect Officer, normally a Chemical Corps officer, must perceive and initially task the OPSEC officer to conduct the vulnerability analysis. After conducting a vulnerability analysis and identifying the MILDEC requirement, the OPSEC officer would go over to the MILDEC planner in G5 Plans to coordinate for a supporting MILDEC plan. Depending on his priorities from the Plans Chief and his concurrence, the MILDEC planner develops the CONOP and then passes the plan to G3 Current Operations for preparing, executing, assessing, and adapting the plan.[25] Implied in this process is the coordination and synchronization, across the other staff elements, the MILDEC planner would undertake. For example, to develop culturally appropriate messaging and dissemination support, he would have to work with the G7 who is responsible for PSYOP staff oversight.[26] If there was a CNO or technical aspect, he then goes to the FSCOORD and G3 Space Branch respectively to coordinate for their support as well. After accomplishing this, he then hands the plan off to Current Operations who has to be capable of discerning all the MILDEC planner's points of contact and nuanced coordination for execution.

If practice in the field is any guide, this contrasting process is unwieldy and not very practicable. Based on MILDEC imperatives that limit access to deception planning and execution, MILDEC planners use top secret systems for planning in a sensitive compartmented information facility (SCIF), separated from Current Operations and manage their own executions. Also, because the coordination has now become a labor intensive task, the hand-off between the G-5 and G-3 exposes the process to risk. Additionally, this scenario assumes that there actually are officers occupying these positions, with training, having these functions as their primary duty, and staff leads knowledgeable of how this all works together. Clearly, the Army's new informational construct introduces increased and undue complexity in generating combined effects from IO capabilities. To be sure, it presents a more daunting and complicated situation for staffs to work through, challenging the notion that this arrangement maximizes IO capabilities for the commander.

[25] Ibid, 186.
[26] U.S. Department of the Army, *Information*, Draft FM 3-13 (Washington, DC: U.S. Department of the Army, 27 February 2009), 6-8.

Another aspect of the new information doctrine that begs examination is the G-7 concept. According to the new doctrine, the G-7 is the staff proponent for IE and is an FA 30 designated position. IE is the integrated employment of Public Affairs (PA) to inform U.S. and friendly audiences; psychological operations, combat camera, U.S. Government strategic communication and defense support to public diplomacy, and other means necessary to influence foreign audiences; and leader and soldier engagements to support both efforts.[27] The G-7 is responsible for chairing the IE working group and is responsible for coordinating, synchronizing, orchestrating, assessing, and adapting the information engagement activities of the constituent elements of IE; harmonizing IE activities with all other lethal and non-lethal means; and integrating IE activities into plans and orders.[28] Personnel from FA 30, PA, and PSYOP career fields staff the G-7. As stated previously, the intent of this construct is to fill the need for a military public relations capability that communicates "effectively and coherently" to all audiences. To begin with, the appropriateness of whether the military should have this function resident in doctrine and organization is questionable. It is instructional to heed the case of the ill-fated Office of Strategic Information (OSI) created by Secretary of Defense Rumsfeld in 2002. OSI shut down in short order amidst a storm of media controversy over the prospect that it would "infuse" information warfare into the media.[29] There were acute concerns within the Pentagon that this would undermine the public credibility of the Department of Defense (DoD) and raised serious questions among journalists whether or not they were being lied to.[30] In a similar fashion, when the media understands that the staff responsible for crafting the communications strategy for the command consists of IO and PSYOP personnel, the perception will be that the intent of this staff is to "*PSYOP*" the public and the media. Intensifying this controversy will be the discovery that there is an actual Army career field whose purpose is to integrate the employment of PA and PSYOP. While the intent of this function is not to deceive the public, it is unlikely that the media and the general public will grasp the subtlety of fine conceptual distinctions. Additionally, we are handing potential adversaries a huge propaganda opportunity by giving them the basis to claim that anything we say is a "lie." To be sure, the G-7 construct will prove to be counter-productive as the credibility of the command will undoubtedly suffer. If the command loses credibility, it loses the ability to communicate effectively.

In addition to credibility problems inherent to the G-7concept, there are also issues related to staff redundancy, friction and the actual value the G-7 provides. Previous to IE and the current G-7 incarnation but still resident in joint doctrine, communications integration occurred through working groups in the Boards, Bureaus, Centers, Committees and Working Groups (B2C2WG) construct, integrated with operations in the targeting and operations-synchronization process. This allows communications strategy development in a collaborative manner amongst staff sections that have distinct functions and responsibilities with no redundancies. Under the new paradigm, the extant purpose of the G-7 is to integrate the PA and PSYOP functions and be the staff proponent for communications strategy. This will most certainly overlap with the PAO's

[27] U.S. Department of the Army, *Operations*, FM 3-0 (Washington, DC: U.S. Department of the Army, February 2008), 7-3.
[28] DA Pam 600-3, 187.
[29] Eric Schmitt and James Dao, "A 'Damaged' Information Office is Declared Closed by Rumsfeld," *New York Times*, February 27, 2002.
[30] Ibid.

(Public Affairs Officer) traditional function and impinge on what the PAO perceives to be his role on the staff. Moreover, the PAO is a special staff member for the commander and has direct access to him while the G-7 works under the supervision of the Chief of Staff (CoS) and does not have direct access. As a result of this overlap of functions and roles, friction in the staff will invariably occur. Given that the G-7 essentially fulfills the function of what is now performed by a working group absent staff overlap and friction, one is left to wonder how much value this really provides the commander.

Another aspect of the new information doctrine that requires examination is the C2W concept. C2W integrates physical, attack, EW, CNO, to degrade, destroy, and exploit the adversary's command and control (C2) system or deny information to it.[31] Structurally, EW and CNO planners residing in the FSCOORD form the C2W cell. Doctrine specifies that while C2W effects are achieved primarily through physical and technical means, PSYOP and MILDEC also provide support.[32] This arrangement neither relates to contemporary OEs nor reflects common practice. The idea of C2W is not new and is a resurrection of a function that is the antecedent of IO from the early 1990s. IO enhanced the C2W concept with the additional synergies realized by adding the "soft" components of PSYOP, MILDEC, and OPSEC. Ironically, the same rationale that Wass de Czege uses against IO can also apply to the C2W concept as it was designed for employment against adversaries in an unconstrained OE from even before the time IO was conceived. Indeed, in today's OE and into the foreseeable future, operations will transpire in a constrained milieu. In an OE that is less than full-scale war and against adversaries that utilize the same information infrastructure for command, control and operations that populations do, the idea of degrading, destroying, and exploiting the adversary's C2 system is fraught with complications. Imagine a scenario in a contemporary environment where we are trying to influence the population to support our objectives and the impact of destroying or degrading cell phone networks, internet connectivity, satellite TV, and terrestrial radio and TV transmissions. One, we would incite anger in the population against us and, two; we would diminish the very means we are using to reach the target audiences. Not to mention the collateral damage we would impose in the surrounding countries and, in the case of CNO and space applications, potentially around the globe. In this scenario and in common practice, EW and CNO capabilities are best suited for and used most often in conjunction with PSYOP, MILDEC and technical applications for counterpropaganda and precision message delivery. The employment of these capabilities as if they were similar to "artillery" is simplistic and counter-productive.

Separating the "hardware" of EW and CNO from the "software" of PSYOP and MILDEC, and OPSEC inhibits the potential to maximize these capabilities. A case in point to illustrate the advantage of developing hardware and software in concert to maximize performance is Apple's design philosophy. Apple computers are widely recognized reputation for superior performance and dependability in contrast to Windows based PCs. Indeed, sales of Apple computers in 2008 outgrew the industry in the last 14 of 15 quarters, its total share of market is 18%, and one of every three dollars spent in retail computer sales is spent on a Mac.[33] This should not come as a

[31] FM 3-0, 7-6.

[32] Ibid.

[33] Researchcast, "2008 Mac Sales Statistics," October 14, 2008, http://www.reasearchcast.com/alpha/?p=101 (accessed May 30, 2009).

surprise, as both software and hardware advance in concert with each other "in-house," to maximize their capabilities as opposed to the separate development of the software and hardware of a PC. In the same way, it makes better sense to bundle capabilities that, when combined together, achieve greater effects than otherwise might be the case if engaged separately. PSYOP and MILDEC, in conjunction with technical capabilities, expand the means available to support their function and, conversely, those technical capabilities provide leverage to maximize their potential and relevancy. Moreover, because of the high degree of complexity in creating these synergies, the training and experience of a multi-skilled coordinator facilitates navigating the labyrinth of authorities, statutory requirements, interagency coordination, as well as the employment of the capability itself, to produce actual effects in the battlespace. It is not realistic to expect similar synergies to occur with IO capabilities dispersed across the staff as the new information doctrine would have it.

The New Information Construct and the Army's Campaign Plan

Another dilemma the new Army information doctrine presents is that it does not support the stated objective of the Army Campaign Plan, which is the creation of a "joint and expeditionary Army with campaign capabilities."[34] According to the campaign plan, the force needs to be able to integrate with the joint force and even brigade level units will be utilizing joint, interagency, and multi-national capabilities.[35] Under the modular force transformation concept, corps and divisions headquarters will form the basis of a joint task force (JTF) or joint force land component command (JFLCC) and, as such, must organize according to and operate within joint doctrine.[36] A separate and distinct Army information doctrine, outside joint doctrine, directly contradicts the intent of the campaign plan as well as modular transformation.

Organized and trained based on Army information doctrine, converting a corps or division designated as a JTF/JFLCC to a joint organization and operating according to joint doctrine will be problematic and difficult. Draft FM 3-13 proposes that the C2W cell in the FSCOORD form the nucleus of the IO cell and draws the PSYOP, MILDEC, and OPSEC personnel from their parent staff sections to reconstitute a joint IO organization. There is certain to be a steep learning curve as these officers will lack prior experience working together and the professional competencies to effectively plan, integrate, and employ IO. Conversion to a joint structure will also disrupt other staff sections as they lose their team members to the reconstituted IO cell. The commander, staff, and B2C2WG process will have to learn how to interact with the new IO cell as much as the IO cell has to learn how to interact with them. In sum, if the Army's objective is to be "joint and expeditionary," the point is lost as to why the Army is spending intellectual energy and resources on an information doctrine whose relevance is questionable and clearly violates a basic Army maxim to "train as you fight."

Inherent to the new paradigm are a number of anomalies that call into question its overall coherence. Two major cases in point are the re-engineered Functional Area 30 and who is actually responsible for planning information operations. Because FA 30 competencies now

[34] Department of the Army, "Worth Fighting For, Army Campaign Plan," briefing slides, Washington, DC, U.S. Department of the Army, accessed 15 February 2009.
[35] Ibid.
[36] FM 3-0, C1-C5.

focus on aspects that relate to creating inform and influence effects, they only receive an ILE-type introduction to the other IO capabilities.[37] Newly certified FA 30s assigned to Army units who have not transitioned to the new doctrine or are in a joint environment, have to receive additional MILDEC, OPSEC, and CNO training to be able to function in the IO cell. The new doctrine also envisions that when FA 30 officers post at joint organizations, where there is not an IE G-7 construct, they will assume IO positions for which they will also lack training. Another example is that there will not be joint IO operators in a re-constituted IO cell while in the G-7 there will most likely be FA 30s with joint IO assignment experience. Further, in the Department of the Army (DA) Pamphlet 600-3, it establishes that FA 30's belong to the Information Operations Functional Area and perform IE while "Field Artillery officers plan and integrate information operations and electronic attack."[38] It would seem that the Army is saying that Field Artillery Officers are now the new IO officers. Divested of information operations, FA 30 becomes a hybrid functional area that offers less capability to commanders and a confused identity and role for current and future FA 30s.

Conclusion

The Army is at a critical fork in the road with respect to the direction of information doctrine. Down one path is a theoretical approach based on rational deduction and analytical propositions whose logical certainty is disconnected from actual practice and experience. Down the other path is a doctrine that provides the foundation on which to build an information doctrine for the future based on capturing experiential knowledge gained from six hard years of operations in Iraq and Afghanistan.

Indeed, reaction from those commanders who have extensive operational experience and who realize the effects IO produces in the battlespace, is noteworthy in their non-concurrence with the draft FM 3-13. Among those commanders who have disagreed with the new direction are the former and present MNC-I commanders, and the current Multi-National Forces- Iraq (MNF-I) and former MNC-I commander, General Odierno.[39] In an ironic twist, General Petraeus, who initiated this "new look" at IO when he was the CAC Commanding General, as Commander, U.S. Central Command (CENTCOM), is creating an IO Task Force in Afghanistan as well as an IO Staff Section at CENTCOM modeled on the MNC-I IO task organization and functions after having served as MNF-I commander. In light of what operational commanders think and what they are doing, CAC would do well to take reconnect its thinking with the field.

To be sure, the Army has been at similar doctrinal crossroads in its history and the lessons drawn from those moments should be instructional to us in the current situation with information doctrine. With the introduction of the tank during WWI, the Army glimpsed of the future of mechanized warfare. After the war, however; the Army closed its eyes to the potential of armored warfare and, mired in bureaucratic branch parochialisms, relegated the tank to the

[37] U.S. Army Information Operations Proponent, *FA-30 Qualification Course*, CD (Ft. Leavenworth, KS: Combined Arms Center, November 2008).

[38] DA PAM 600-3, 93.

[39] LTG Austin was briefed on the Draft FM 3-13 on 2 April 2009 and non-concurred with the draft and sent an email to the CAC commander. GEN Odierno was briefed on Draft FM 3-13 on 12 April 2009 and strongly non-concurred and sent an email to the TRADOC commander.

Infantry Branch and "light" armored vehicles to the Cavalry Branch. Development of mobile armored warfare was stifled as armor was employed according to the prevailing mental models of the branches to which they were apportioned. It wasn't until the stunning success of the German "blitzkrieg," which demonstrated the efficacy of combined arms in mobile armored formations, that the Army re-evaluated its doctrine and organization. Today, we face a similar situation with respect to whether or not we grasp the potential of the combined effects achieved through the fusion of hardware with software the IO paradigm offers rather than succumbing to bureaucratic impulses. In the novel "To Kill a Mockingbird," on giving air rifles to his children for Christmas, Atticus Finch admonishes them that while they can shoot blue jays all they want, they should not shoot mockingbirds because they are innocent. Likewise, the Army should not deconstruct the IO paradigm but build on it.

Colonel Randolph Rosin is currently serving as the I Corps/MNC-I Information Operations Chief. He is a Middle East Foreign Area Officer by trade but was a Psychological Operations Officer for 9 years and served as the PSYOP Officer/Deputy IO chief at CENTCOM 2000-2003.