Fighting Terrorism and Insurgency: Shaping the Information Environment

Major Norman Emery, U.S. Army; Major Jason Werchan, U.S. Air Force; and Major Donald G. Mowles, Jr., U.S. Air Force

And let there be no doubt, in the years ahead it is likely that we will be surprised again by new adversaries who may also strike in unexpected ways.—Donald H. Rumsfeld[1]

IN ISKANDARIYAH, Iraq, approximately 30 miles south of Baghdad, a bomb exploded at a police station, killing 50 Iraqis applying for the new police force. U.S. forces conducted operations to seek out and defeat those responsible. Often, U.S. forces are successful in finding, engaging, capturing, or killing insurgents who instigate terrorist attacks. However, this traditional attrition-based approach to counterinsurgency does not adequately address its strategy and secondary effects.

By attacking the police station, Iraqi insurgents hoped to achieve their strategic objectives of influencing Iraqi perceptions about security and safety; contributing to the delay or cancellation of free elections; de-legitimizing an interim Iraqi government; and degrading domestic support for U.S. policy in Iraq. This scenario demonstrates the limitation of U.S. joint information operations (IO) doctrine in addressing a new approach to warfare. Nonstate actors such as terrorists and insurgents will likely be the major threat to U.S. national security and its interests for years to come. Because these actors cannot directly confront the U.S. militarily, they must rely on an information advantage to marginalize U.S. capabilities.

Over the past decade, various high profile terrorist groups have demonstrated a sound knowledge and coordinated use of information operations. Their ability to successfully achieve objectives by shaping their battlespace in the information environment, coupled with willingness to conduct nontraditional warfare, make them a significant threat to the United States.

Although the initial Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations*, addresses a traditional IO approach against conventional forces such as China or North Korea, it does not sufficiently consider nonstate threats such as terrorists and insurgents.[2] The joint staff is currently updating JP 3-13 by incorporating the October 2003 revised Department of Defense (DOD) IO policy, informally known as the secretary of defense's (SECDEF's) "IO Roadmap."[3] To succeed in the new security environment, JP 3-13 must provide an IO approach that better defines and shapes operations in the information environment (IE) to enable victories over nonstate actors in the physical environment (PE).

Current and Future Security Environments

The United States is facing a drastically different security environment than it faced before 11 September 2001. In the past, adversaries confronted the United States with conventional armed forces backed by the industrial capabilities of a nation-state. Today, a single nonstate actor or terrorist group can attack the Nation and create untold destruction.

The *U.S. National Security Strategy (NSS)* defines a new security environment that includes these terrorist organizations and the nation-states and organizations that harbor them: "[T]he United States and countries cooperating with us must not allow the terrorists to develop new home bases. Together, we will seek to deny them sanctuary at every turn."[4]

Terrorism took many forms after 11 September 2001, but the United States is primarily concerned with terrorists who possess a global strike capability and whose global reach makes them extremely elusive and difficult to define or engage. In response to this new security environment, SECDEF Donald H. Rumsfeld changed the military strategy in the 2001 *Quadrennial Defense Review (QDR)* from a threat-based approach to a capabilities approach to better respond to the numerous threats the United

States faces.[5] By adopting this approach, defense planners can concentrate on how a potential enemy might engage the United States rather than concerning themselves with who that enemy is or where he will attack.

Joint IO Doctrine

Numerous documents provide direction of overall joint IO strategy, including JP 3-13, *Joint Vision (JV) 2010*, *JV 2020*, and the recently published "IO Roadmap."[6] Joint Publication 3-13 provides doctrinal guidance for joint forces information operations. The 1996 *JV 2010* defines information operations as "[a]ctions taken to affect adversary information and information systems while defending one's own information and information systems." *Joint Vision 2010* sets forth "a vision for how the United States military will operate in the uncertain future" and achieves the ultimate goal of full-spectrum dominance.[7]

Information superiority is a key element of full-spectrum dominance. *Joint Vision 2010*, which states that information superiority will mitigate the effect of the friction and fog of war, advocates ensuring an uninterrupted flow of information and nontraditional actions. *Joint Vision 2020* adds: "The combined development of proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control."[8]

The "IO Roadmap" provides strategic-level IO guidance for the current security environment defined in the latest *QDR* and *NSS*. The draft update of JP 3-13 incorporates the "IO Roadmap" and a new DOD IO definition: "The integrated employment of the specified core capabilities of Electronic Warfare [EW], Computer Network Operations (CNO), PSYOP [psychological operations], Military Deception, and Operations Security [OPSEC], in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decisionmaking, while protecting our own."[9] The "IO Roadmap" groups IO elements in the following categories:

- Core capabilities (EW, CNO, OPSEC, military deception, PSYOP).
- Support capabilities (information assurance, physical security, counterintelligence, physical attack).
- Related capabilities (public affairs, civil-military operations).[10]

Although current and draft IO doctrine encompasses many aspects of warfare, the ability to deal with the new security environment still needs scrutiny. The new definition focuses offensive information operations against the adversarial decisionmaker, ignoring that there are many valuable targets in the information environment that are not critical decisionmakers. The 1998 definition of information operations was so broad that it was everything and yet nothing.[11] The new draft definition limits itself in applying information operations to the listed core capabilities.

US Army

Iraqi police search for clues after detonation of a car bomb near Baghdad's Al-Rasheed Hotel, 4 December 2004.

Joint Publication 3-13 poorly defines and applies the concept of information superiority as it would apply to a nonstate actor. Information superiority is an imbalance in one's favor in the information domain with respect to an adversary. The power of superiority in the information domain mandates the United States achieve it as a first priority, even before hostilities begin. However, superior technology and equipment fuels hubris to have information superiority over inferior adversaries.

A nonstate actor can decisively possess information superiority and an information advantage because he can remain unseen in his own environment, yet see U.S. forces, and choose when to attack.

U.S. information superiority can be finite and fleeting; its forces must recognize this and take direct and indirect action to reduce the adversary's information advantage and operational efficiency. Information superiority in the new security environment must include denying information helpful to a nonstate actor by reducing OPSEC violations and information the population can provide.

Physical Environment v. Information Environment

Nothing is more important when conceptualizing joint IO doctrine in the new security environment than understanding the relationship between the physical environment and the information environment and how the United States should approach information operations in these areas against a nonstate actor. Joint Publication 3-0, *Doctrine for Joint Operations*, defines the physical environment by the dimensions of land, sea, air, and space.[12] Humans live, breathe, and walk in the physical environment, and they see, hear, and touch objects that are real.[13] Leaders generally conceive and measure gains and losses in the physical environment by the metrics of terrain, equipment, forces, and engagements.

According to the draft JP 3-13, the information environment consists of information that resides in the mind, physical world, and electromagnetic spectrum.[14] Boundaries are "not limited to the linear battlespace that military commanders conceptualize, [and] activities in the information environment often shape a commander's understanding of the battle and can profoundly affect his decisions in the physical environment."[15] For example, forces providing security to a population is an act in the physical environment, but the population's perception of security is in the information environment. Military leaders and planners must understand that the PE and IE domains exist in simultaneous yet separate battlespaces. Nonstate actors operate mainly in the information environment to leverage their advantage, and states tend to operate in the physical environment to achieve their goals. The United States must adapt its approach to conflict to maximize its results while diminishing the adversary's.

Another key IE and PE characteristic is that "wherever human activity occurs physically, such activity [also] takes place simultaneously in the information dimension."[16] This is important in recognizing those residual effects from actions taken in the physical environment that will shape the information environment. Draft JP 3-13 fails to address factors that shape the information environment in which military operations are planned and executed or recognize that success depends on U.S. forces gaining and maintaining information superiority.[17] However, previous IO doctrine and U.S. operations have traditionally sought to achieve finite victory in the PE battlespace and ignore the concurrent residual effects in the IE battlespace.

Current and draft joint IO doctrine fails to adequately explain and emphasize the information environment and the art of its application against U.S. adversaries. The key to preparedness against current and potential security threats, such as nonstate actors, lies in the art of information operations, not just the science. The science of information operations can be the application of systems and capabilities to support the goal of affecting adversary decisionmaking at a specific moment in time and space, while the "art focuses on the fundamental methods and issues associated with synchronization of military effort" in the information environment.[18]

Draft JP 3-13 says: "Operational art is the use of military forces to achieve a strategic goal through the design, organization, integration, and conduct of strategies, campaigns, major operations, and battles."[19] To fight a nonstate actor whose operational actions are planned to achieve strategic goals, the United States must operate similarly. U.S. planners must apply all facets of operational art in the information environment and the physical environment. There is more to information operations than just affecting adversary decisionmaking as proposed in the draft definition; coordinated military actions must affect the information environment as a whole.

Although draft JP 3-13 establishes the IE's conceptual context and military operations related to it, it does not address the need to shape that environment because of friendly or adversary actions in the physical environment. The United States enjoys a force advantage over most of its adversaries and, therefore, seeks objectives and victories in the physical environment using actions in the information environment as an enabler.

In contrast, terrorists and insurgents, who lack military parity, seek to achieve their ultimate objectives by being successful in the information environment. They cannot successfully engage a superior force in the physical environment, so they conduct selected acts in the physical environment (bombings and small-scale attacks, for example) to shape the information environment (that is, perceptions). These acts can help achieve objectives in the information environment and, ultimately, in the physical environment. Therefore, a nonstate actor might choose to

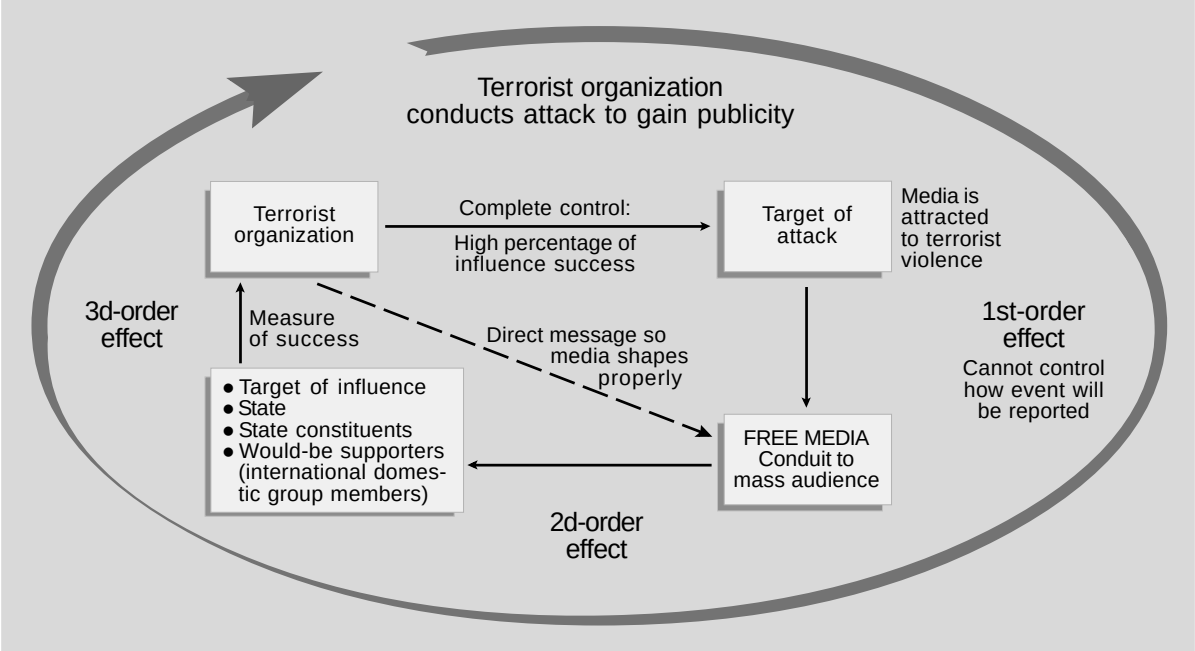

Figure 1. McCormick Influence Process Model.

avoid a decisive fight with U.S. forces, selecting instead a more advantageous time and location for engagements. Nonstate actors will avoid direct confrontation in a state's PE battlespace, but a state actor can defeat them by reshaping their information environment.

How to Pursue Victory

Current doctrine directs U.S. forces to achieve a decisive victory in the physical environment while using the information environment to support "objectives and reduce costs of war."[20] Although U.S. information operations might often affect the adversary's perception or will to fight, the United States normally relies on victory in the physical environment to win the battle, which is a typical strategy of a military with a force advantage over the majority of its adversaries.[21]

Joint doctrine supports this by orienting on affecting adversary decisionmaking to influence decisions in the United States's favor and to prevent the adversary from influencing U.S. forces. While this approach is adequate for a conventional adversary such as North Korea, it is inadequate for nonstate threats such as insurgents and terrorists. The United States might understand how to strategically shape the information environment, but at the operational level it often relies on its superior military might or its force advantage to achieve victory in the physical environment, neglecting the efficient, effective use of the information environment.

How Terrorists and Insurgents Pursue Victory

Terrorists and insurgents adopt a much different approach to achieving victory through the use of a complex IO strategy. They develop the IE battlespace because of the benefits gained from its residual effects. In *The Terrorist Approach to Information Operations*, Norman Emery and Rob Earl say: "Terrorists act in the physical environment not to make tactical gains in the physical environment, but to wage strategic battle in the information environment; therefore the physical environment enables many of the activities in the information environment to occur."[22]

Figure 1 shows the model nearly all terrorists follow to achieve objectives by indirectly influencing a decisionmaker.[23] The process applies to select insurgencies. The model's four steps and three orders of effects begin with a bombing or attack in the physical environment that the media or members of a population report. The interpretations can shape perceptions of a populace or government in the information environment. Terrorists then determine follow-on actions in the physical environment depending on the measure of success in the information environment. Perceptions once developed can endure for days, months, or decades and are difficult to change.

The model demonstrates that a specific act in the physical environment produces residual effects and

offers an approach for U.S. forces to interdict the adversary's information environment to reduce or reverse the effectiveness of PE actions. Therefore, any operation to eliminate nonstate actors and their influence must also employ forces operationally to counter the potential strategic effect and results of previous nonstate operations. Having effective counteroperations to current and previous acts in the information environment, not just attrition warfare in the physical environment, is important. Shaping the information environment is not merely denying information to adversary decisionmakers; it is denying them results from their actions.

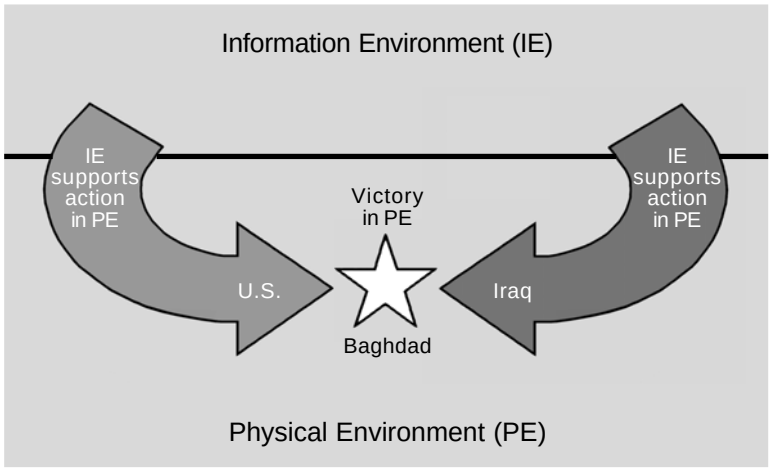

Figure 2. Application of information operations in conventional conflict.

The big difference between what current U.S. doctrine is and should be is in its approach to conflict. As long as U.S. forces are denying a state foe his ability to make a decision, they are shaping his information environment. The United States might not be able to affect a nonstate foe's ability to make a decision if he maintains an information advantage, but it can affect his results in the information environment, his chosen battlespace. As long as the United States conceptualizes all victories in the physical environment through decisive engagement rather than more lengthy action in the information environment, it might not succeed as quickly. If the United States adjusts its approach to nonstate conflict, it can beat insurgents and terrorists at their own game in their own battlespace, which requires a new approach to modern conflict.

The Art of Information Operations

Figures 2 and 3 illustrate the U.S. military's current approach to state and nonstate conflict, which works when engaging a similarly structured adversary such as North Korea or Iraq in linear conventional warfare. Figure 2 shows conventional-force actions in the information environment, such as PSYOP campaigns, EW, deception, and OPSEC measures supported by media messages and civil-military operations to achieve victory in the physical environment.

The problem with the approach in figure 2 is it does not work against such nonstate actors as insurgents or terrorists, who operate by design in a different battlespace. Figure 3 concerns the Iraqi police station bombing vignette and shows how state and nonstate forces can operate in different battlespaces with the nonstate force gaining the long-term advantage.

U.S. forces conduct operations in the physical environment to defeat or deter Iraqi insurgents responsible for a series of bombings; however, that is only a portion of the insurgent's battlespace because they shaped the information environment with residual effects from previous attacks. The attacks on Iraqi supporters of U.S. programs perpetuate insecurity in the fearful population, a perception which does not dissipate with a few U.S. force victories against insurgents. The perception reaches audiences in the information environment, which ultimately supports insurgents' strategic objective in the physical environment, such as

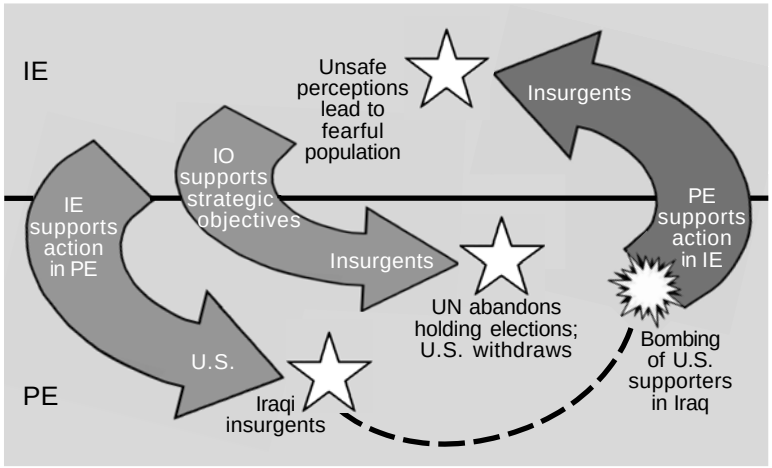

Figure 3. Strategy for nonstate conflict.

forcing the UN to cancel elections or the United States to withdraw prematurely.

To win, the United States must realize and employ the art as well as the science of information operations. The United States must also understand that when its forces react negatively and kick down doors in night raids, they are helping the enemy improve his own information environment. Their actions will annoy and alienate citizens who might no longer cooperate or who might begin actively supporting the insurgents. A silent population is de facto support to insurgents, who maintain or increase their information advantage in the information environment.

The effect insurgents have on the information environment is comparable to the ripples that dropping a large stone into a lake causes. Long after the stone has hit the bottom, the residual effects expand in all directions, are difficult to stop, and ultimately crash into the banks of the lake. Current U.S. counterinsurgency strategy focuses on the splash of the stone (the PE), and not enough on stopping the ripples (the IE) before they reach the bank—the enemy's strategic PE objective.

Recommendations

Revisers of the next draft of JP 3-13 should consider the recommendations in the following paragraphs to improve the U.S. military's ability to counter nonstate threats.

The doctrinal definition of IO needs to be modified to better reflect operations in the information environment. The proposed IO definition in the draft JP 3-13 limits what we can accomplish by limiting what capabilities we can use. Information operations are the effects sought, not just tools to get these effects. The new definition should emphasize using all available capabilities in full-spectrum operations to affect the information environment instead of focusing solely on the adversary's decisionmaking capability in the physical environment. The IO definition we recommend is: "The timely employment of specified capabilities to influence, disrupt, corrupt, or usurp the adversarial information environment and decisionmaking while protecting our own."

The next recommendation is to emphasize information operations to influence and obtain information superiority. The United States must break the mindset that information superiority is an inherent part of combat superiority. The most powerful force might not always have information superiority or the ability to directly influence adversarial decisionmakers to shape the information environment. To achieve information superiority, IO doctrine should address actions in the information environment to enhance U.S. objectives against nonstate actors who rely on the information environment as their primary battlespace.

We also recommend emphasizing the art of information operations as one of the core concepts of offensive information operations. The joint community has a prime opportunity to shape a new approach to warfare by addressing actions and effects in the information environment, not just in the physical environment, to enhance effects against nonstate actors who rely on the information environment as their primary battlespace.

Last, we recommend IO doctrine change its approach to nonstate threats by conducting find, fix, and finish actions in the physical environment while shaping residual effects from previous actions in the information environment. An adversary's residual effects might persist from previous actions in the information environment following some act in the physical environment. To counter this, U.S. IO doctrine should adopt a simultaneous two-pronged approach against nonstate threats through physical attacks as well as through disrupting and minimizing their current and previous influence in the information environment (figure 4).

Draft JP 3-13 briefly addresses principles that would support the two-pronged approach but insufficiently emphasize it as a core concept and says the focus of offensive information operations is to directly affect information to indirectly affect decisionmakers "by taking specific psychological, electronic, or physical actions to add, modify, or remove information itself from the environment of various individuals or groups of decisionmakers."[24] The simultaneous approach reduces nonstate actors'

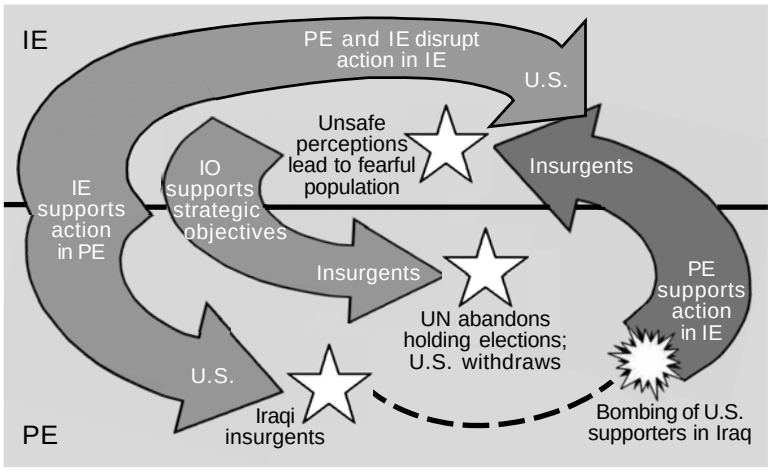

Figure 4. Proposed strategy for nonstate conflict.

operational effectiveness and support, causing them to either decrease operations or take greater risks in their activity, thereby increasing their exposure to defeat in the physical environment.

Succeeding in the Security Environment

Current published or draft joint IO doctrine insufficiently addresses nonstate conflicts the United States now faces. To succeed in the new security environment, the new JP 3-13 must better define IO- and IE-shaping operations to enable ultimate victories in the physical environment. Military leaders and planners must understand that while PE and IE domains coexist, they are separate battlespaces. Nonstate actors operate mainly in the information environment to leverage their advantages, while the United States often chooses to leverage its force advantage in the physical environment.

Fighting nonstate actors such as terrorists and insurgents requires an understanding of the residual effects of gains and losses in the information environment based on actions in the physical environment. The benefit of the residual effects in the information environment from actions in the physical environment are far greater than the physical result from the act (that is, deaths from a bombing). To combat these residual effects, the United States should seek to shape the information environment in its favor by conducting simultaneous operations to find, fix, and finish in the physical environment while shaping residual effects in the information environment from current and past adversary and friendly actions in the physical environment.

Shaping the information environment requires a new way of thinking and a new staff approach to warfare, with planners and leaders conceptualizing nonstate conflict differently than traditional conflict. The military should not continue to inadequately address an important dynamic in current and future warfare. Planners must not get caught up in seeking immediate effects while ignoring the value of gaining effects in the information environment, because the results there are slow in coming and difficult to quantify. Military operations do not always produce tangible, visible, or immediate effects. By shaping the information environment, military forces can affect the enemy decisionmaker by influencing his environment without changing his perception or decision.

This battle of ideas requires more bytes than bullets. The military can achieve this by using the science of information operations to focus on decisionmaking in the physical environment and using the art of information operations to shape the information environment; this synchronization achieves the victory in the physical environment and counters results in the information environment from current and previous actions in the physical environment. As long as U.S. information operations orient solely on the PE victory, the U.S. cannot successfully engage and defeat the wide range of threats in the ever-changing security environment. ***MR***

NOTES

1. U.S. Secretary of Defense Donald H. Rumsfeld, *Joint Operations Concepts* (Washington, DC: U.S. Government Printing Office [GPO], November 2003).
2. Joint Chiefs of Staff (JCS), Joint Publication (JP) 3-13, *Joint Doctrine for Information Operations* (Washington, DC: GPO, 1998).
3. U.S. Department of Defense (DOD) IO policy ("IO Roadmap"), Washington, D.C., October 2003.
4. The White House, *National Security Strategy of the United States* (Washington, DC: GPO, 2002).
5. DOD, *Quadrennial Defense Review* (Washington, DC: GPO, 30 September 2001).
6. JP 3-13; JCS, *Joint Vision 2010* (Washington, DC: GPO, 1996); *Joint Vision 2020* (Washington, DC: GPO, 2000), 28; "IO Roadmap."
7. *JV 2010.*
8. *JV 2020,* 3.
9. JP 3-13 (draft), I-6.
10. "IO Roadmap."
11. Edwin Armistead, ed., *Information Operations: The Hard Reality of Soft Power* (Washington, DC: National Defense University, 2002).
12. JP 3-0, *Doctrine for Joint Operations* (Washington, DC: GPO, 2001).
13. Rob Earl and Norman Emery, *Terrorist Approach to Information Operations* (Monterey, CA: Naval Postgraduate School, 2003).
14. JP 3-13 (draft), I-2.
15. Earl and Emery, 19.
16. JP 3-13 (draft), I-2.
17. Ibid., I-4, I-5.
18. Ibid., I-10.
19. Ibid.
20. Earl and Emery, 44.
21. Janos Radvanyi, ed., *Psychological Operations and Political Warfare in Long-Term Planning* (New York: Praeger Publishers, 1990), 121.
22. Earl and Emery, 44.
23. Ibid., 11-12.
24. JP 3-13 (draft), I-9.

Major Norman Emery, U.S. Army, is a Functional Area 30 information operations planner assigned to Multinational Forces-Iraq. He received a B.A. from Illinois State University, an M.S. from the Naval Postgraduate School, and is a graduate of the U.S. Army Command and General Staff College (CGSC) and the Joint Forces Staff College. He has served in various command and staff positions in the 3d Infantry Division, the 101st Airborne Division, the 229th Military Intelligence Battalion, and Special Operations Command. His article "Information Operations in Iraq" appeared in the May-June 2004 issue of Military Review. *He can be contacted at norman.emery@us.army.mil.*

Major Jason Werchan, U.S. Air Force, is an instructor with the Air Force Element at CGSC, Fort Leavenworth, Kansas. He received a B.S. from Texas A&M, an M.A. from Oklahoma University, and is a graduate of the Joint Forces Staff College.

Major Donald G. Mowles, Jr., U.S. Air Force, is the Chief, Intercontinental Ballistic Missile Strike Team, Combat Plans Division, U.S. Strategic Command, Offutt Air Force Base, Nebraska. He received a B.S. from Arkansas State University, an M.S. from Central Michigan University, and is a graduate of the Joint Forces Staff College.