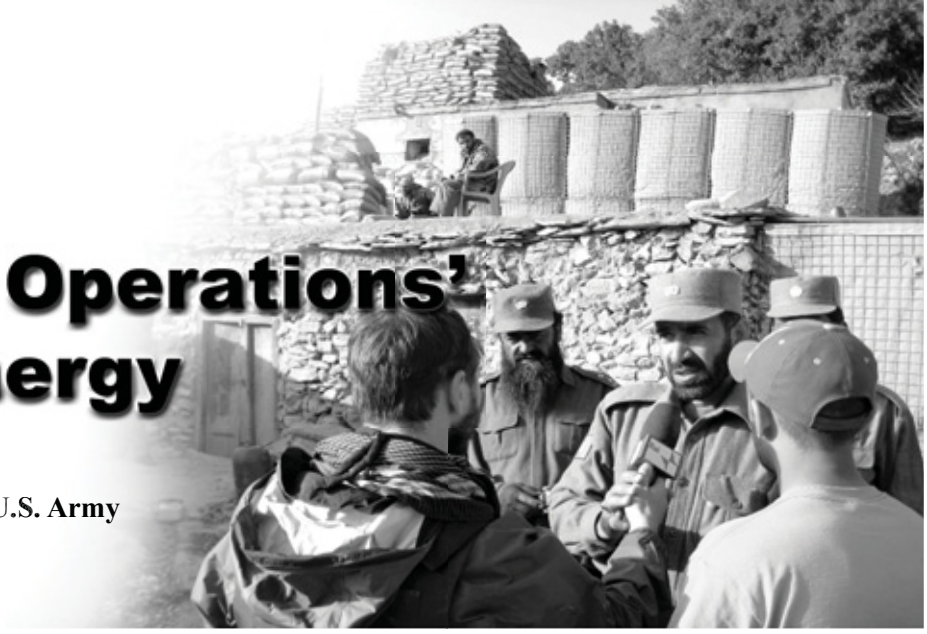
Harnessing Information Operations' Potential Energy



Captain Leonardo J. Flor, U.S. Army

AS A COMPANY commander in Afghanistan, I operated from Asadabad, the provincial seat of Kunar Province. My company worked extensively with our partnered provincial reconstruction team, the provincial governor, the provincial chief of police, and local Afghan media during information operations (IO).

Task Force (TF) Rock, my battalion task force, commanded by Lieutenant Colonel William Ostlund, operated in an extremely violent area of Afghanistan that included Wanat, the Korengal Valley, the Pech Valley, and a shared border with Pakistan's Bajuar Agency. In this area of operations, our TF quickly learned that while we could win any kinetic engagement, we were initially unprepared to execute information operations with equal ability. In our second full month of the deployment, our Alpha company air assaulted into the Watapor Valley and precipitated a fierce engagement that left dozens of insurgents dead and killed two paratroopers. At the end of the day though, we had won the engagement, but we quickly lost the information operations battle. During the battle, insurgents had used a single satellite phone to tell local media that we had indiscriminately killed dozens of civilians. Instead of exploiting a tactical victory, we were instantly on our heels, explaining to the population and our own headquarters that it was all untrue.

From that initial failure, our task force set out to ensure that we would not have another defeat snatched from the jaws of victory due to a lack of aggressive information operations. For the next year, our information operations became tactical-unit battle drills that we executed with vigor as we sought to connect every event to the larger narrative of our counterinsurgency campaign. The result was a more coherent and effective counterinsurgency effort. That focused information operations on the decisive point: the Afghan population.

Having had time to reflect on that deployment, I now see how our initial unpreparedness was symptomatic of a larger doctrinal and structural issue, and that the solutions we developed could be useful in solving what I believe is likely a wider Army information operations problem. Current struggles with how to deal with noncombatant deaths due to air strikes highlight the difficulties that units at every echelon have in harnessing information operations to support counterinsurgency efforts. This article is the product of that reflection.

Captain Leonardo J. Flor, U.S. Army is currently the operations officer of 2d Battalion, 357th Infantry (Training Support), Fort Lewis, WA. From May 2007 to August 2008 he was in Kunar province in Afghanistan commanding Headquarters and Headquarters Company, 2d Battalion, 503d Infantry, 173d Airborne Brigade Combat Team. He served as an infantry platoon leader in Iraq from 2003 through 2004. CPT Flor received a B.S. from the United States Military Academy.

PHOTO: Border Police being interviewed in Afghanistan. Photo courtesy of COL William B. Ostlund

Enhancing the understanding and execution of effective counterinsurgency demands that commanders overcome a doctrinal gap and top-heavy structure of the Army's existing information operations system. Operational commanders must provide their tactical formations—squads, platoons, companies, and battalions—with the commander's intent, delegated decision authority, training, and responsive resourcing to wage persistent, precision information operations with audacity and vigor at the decisive point: the population. Tactical leaders must recognize that tactical IO are a decisive warrior task. Success of the counterinsurgency mission requires their aggressive cultivation of the ethos, principles, and techniques of tactical information operations. The principles and techniques they develop may become the foundation for a more effective and appropriate IO doctrine.

The Doctrinal Gap

No doctrine exists for the employment of IO at the battalion level and below. Information operations in counterinsurgency suffer from a disparity in the definitions of the term as it is understood by the strategic and operational entities that resource and enable IO and the tactical units that can most effectively employ them. As a result, a doctrinal gap has opened between those best positioned to execute IO in counterinsurgency and those best resourced and trained to execute information operations in counterinsurgency. That doctrinal gap manifests itself in diminished understanding and effectiveness of a decisive line of operation.

For tactical maneuver units executing counterinsurgency, the term *information operations* has a vernacular definition roughly equivalent to *public affairs* or *public relations*: "Ensure that we IO this operation and highlight that local security forces are in the lead." This definition of the term is far narrower than that in Joint and Army doctrine. Field Manual (FM) 3-24, *Counterinsurgency*, lists the Joint and Army definitions of information operations as—

> Joint: The integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt, or usurp adversarial human and automated decision making while protecting our own. (Joint Publication 1-02)
>
> Army: The employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception, and operations security, in concert with specified supporting and related capabilities, to affect and defend information and information systems and to influence decision making. (FM 3-13)

These disparate understandings of what IO means capture the nature of the doctrinal gap. The Army built its information operations system to meet the needs of the Army's definition, but it fails to meet the needs of the event-driven definition developed by the tactical formations that execute counterinsurgency at the decisive point. Put more bluntly, the Army is ineffective at information operations in counterinsurgency because the Army did not build its IO system with counterinsurgency in mind.

An effective definition of information operations must also include public affairs, public relations and host nation, military, and domestic media integration.[1] Public affairs and public relations include the use of traditional and nontraditional media and social organizations to distribute information and deliver messages to the population, including the most basic form of IO, getting out and talking to the people, face to face.

Field Manual 3-13, *Information Operations: Doctrine, Tactics, Techniques, and Procedures,* states that the FM is most applicable to corps and divisions:

> The primary users of this manual are ASCC [army service component command], corps, division, and brigade commanders and staff officers—specifically the G-2, G-3, G-7, and staff representatives for military deception, electronic warfare, operations security, fire support, psychological operations, civil affairs, and public affairs. Battalions normally execute higher headquarters IO. In stability operations and support operations, they may be given IO assets. Thus, they need to know their role in brigade and division IO.

No supplementary FM or other doctrine is targeted to inform commanders and leaders at battalion level and below on the effective integration of IO at the tactical level.

Photo Courtesy of COLKunar PRT

Afghan Provincial governor and military personnel give an interview to local media.

Field Manual 3-24 states that "IO may often be the decisive logical line of operation," but that even when they are not, they make significant contributions to setting the conditions for success of all other [logical lines of operation]." Field Manual 3-24 and the military's combat experience over the last seven years also make it plain that the decisive point of a counterinsurgency is the host nation population. Squads, platoons, and companies that live (and die) amongst the population win or lose at counterinsurgency. Given the combat-earned understanding that information operations are at least key to a successful counterinsurgency, it is conspicuous that neither the Joint nor the Army definition of IO is useful to the company commander or fire-team, squad, or platoon leaders who execute counterinsurgency at the decisive point.

The Structural Problem

The existing information operations system concentrates experts, resources, and decision makers at the division and brigade levels, but counterinsurgency demands persistent, responsive IO effects at the company and platoon levels.

Information operations are key to a successful counterinsurgency, and at the tactical level, effective counterinsurgency requires persistent partnership and collocation with the host nation population by units at the battalion level and below. No doctrine exists for the implementation of integrated IO at these echelons, the very echelons where we most need them. Further aggravating the lack of IO doctrine at the battalion, company, platoon, squad, and team levels is a corresponding lack of resourcing, staffing, equipping, and training at these echelons. Instead, information operations enablers and decision makers often reside at the brigade or division levels because that is where the preponderance of manning, equipping, funding, and training is. While brigades and divisions could doctrinally be tactical formations, the contemporary operating environment, shaped by the necessity of maximum tactical exposure to the population, means that brigades and divisions are often functionally operational or strategic. As a result, the locus of the IO delivery system resides at the operational or strategic level while that system's highest pay-off targets exist at the tactical level.

Some of this top-heaviness may be attributable to the nature of some information operations component capabilities. Certainly, capabilities like electronic warfare and network operations should not fall into the scope of responsibility of infantrymen in the close fight. Yet other component capabilities, like public affairs, military deception, and psychological operations, can only be effectively controlled at the tactical, on-scene level. On-scene control of IO is urgently needed in a conflict where increasing the population's confidence in the host nation government is more important than the maneuver of formations. Local understanding, relationships, and IO are essential to the local successes that effective counterinsurgency requires. In the dispersed and distributed counterinsurgency environment, divisions and brigades do not have the local, tactical exposure necessary to achieve these local effects. The Army has yet to adjust its IO system to complement the adaptations its fighting formations have employed to increase success: maximum tactical exposure to the host nation population.

Recommendations

From May 2007 to August 2008, Task Force Rock's counterinsurgency operations in the Kunar and Nuristan provinces of Afghanistan yielded ten principles of information operations that helped overcome the doctrinal gap and structural shortcomings that resulted in an initial lack of readiness to employ aggressive, fully integrated information operations in concert with security, development, and governance efforts.

1. Credibility is the currency of counterinsurgency: "The truth is an asset, not a liability." The assertion that insurgents have an insurmountable advantage in information operations because they are not burdened with honesty is as wrong as it is pervasive. Dishonesty can only be effective in information operations when it goes unchallenged. A durable and effective counterinsurgent IO campaign demands aggressive honesty, both in communicating messages to the population and in addressing insurgent information operations. Tactical units must exploit every opportunity to publicly demonstrate when insurgent information operations are dishonest. Similarly, counterinsurgents must be equally aggressive when admitting their mistakes. If not, the insurgents will gladly take that opportunity to discredit the counterinsurgents and the host nation government every time. Honesty, responsiveness, and effectiveness enable credibility, and credibility with the population is the currency of counterinsurgency.

2. Establish an overarching narrative: "Stay on message." No event in counterinsurgency is discrete. Every event occurs in the context of the larger counterinsurgency effort, and effective information operations are essential to enable the host nation population to understand how this is true. Effective IO explains how every event is part of a larger narrative designed to convince the host nation population to view the government as a preferable alternative to the insurgency. In designing this narrative, counterinsurgents must identify a few simple, resounding themes and then aggressively integrate them into how every event is reported to the population. The insurgents must be "they," while the counterinsurgents and the population are "we."

We must not dismiss these seemingly subtle differences in tone as semantics. We can report an improvised explosive device as "destroying a coalition vehicle and killing two Soldiers," or as "killing two soldiers and disrupting the host nation patrol guarding a road construction crew as they worked to connect a remote town and its farmers to the nation's network of roads and markets." We must explain every event in the context of the narrative—doing so implicitly links the population's future with the efforts of the counterinsurgents, leaving the insurgents to act against that union. Failing to explain how *every* event relates to the narrative cedes control of that event's impact to the insurgents. It is not enough simply to tell the population that something happened. We must tell the population how it affects them and why they should care.

We must explain every event in the context of the narrative.

3. Maintain continuous contact*:* "Every SIGACT [significant activity] is pregnant with IO possibility."

Every significant activity that benefits or hurts the counterinsurgent force contains potential energy that either the counterinsurgents or the insurgents will harness or dissipate. Effective IO requires aggressive counterinsurgent action to maximize the realization of potential energy while minimizing the insurgents' ability to realize their energy.

Too often, counterinsurgent IO only reactively mitigate insurgent information operations. Opportunities to conduct IO are always present, but realizing this requires leaders who understand how to tie every event (or the lack of events) into the larger narrative of the counterinsurgency campaign, and then to reinforce that narrative at every opportunity by every means available. By realizing and capitalizing on the potential energy every significant activity can release, a tactical unit can maintain continuous contact with the population and force the insurgents to react defensively (and therefore be less credible). Counterinsurgents must act aggressively to "turn every setback into a victory, and every victory into a resounding triumph."[2]

In addition, if executed in partnership with local government, media, and power brokers, the persistent presence of information operations can build a habit of information consumption. The host nation population's willingness to side with the insurgents may be less because of religious, tribal, or cultural sympathy than the lack of a reliable and persistent source of information. When a persistent, alternative narrative piques the population's demand for information, the host nation population can make better-informed decisions on the merits of the government and the insurgency. The emergence of

Photo Courtesy of COL William B. Ostlund

Ground breaking ceremony in Task Force Rock's area of responsibility.

a persistent, alternative narrative can help incentivize more host nation media to meet the demand. Multiple information sources can be a sign of a functioning government.

4. Gain the initiative: "You don't have to be right; you have to be first and not wrong."[3] The counterinsurgent force must "break" the story to the population before the insurgents do. Our IO culture often values accuracy over responsiveness, but that is a false choice. Accuracy and responsiveness are not necessarily mutually exclusive. Honesty does not imply inertia. Being "not wrong" is different from being "right." The space between those two standards has more to do with completeness than accuracy. Credibility does not require immediate completeness, but it does demand accuracy, responsiveness, and eventual completeness. It is neither acceptable nor effective to mislead, lie, or withhold information (except for the purposes of operational security or military deception), but that does not mean that it is acceptable to wait until everything is known to do something. Leaders must be able to operate in the space between rushing to failure with *insufficient* information and waiting until failure for perfect information. That same balance is required every time a tactical unit reacts to kinetic contact, so the precedent for junior leaders thriving in that space exists. A partial explanation (it does not have to be complete, it just can't be wrong) and a plan to move forward delivered within minutes translates into more credibility with the population than does the 100 percent solution delivered two weeks later.

5. Mass effects at the decisive point: "Employ population-centric IO." In counterinsurgency, the decisive operation's purpose should always be population-centric. For a force trained primarily in the kinetics of combat, the habit is to employ IO only to counter the insurgents' IO because the

Being "not wrong" is different from being "right." The space between those two standards has more to do with completeness than accuracy.

decisive point in kinetic operations is normally enemy-centric. Units often target their information operations on the insurgents rather than the population because they are used to massing effects on the enemy. The decisive point in counterinsurgency is the population, not the enemy. It may be the case that a shaping effort targets the insurgents, but just as in kinetic operations, the shaping purpose must nest within the purpose of the decisive operation.

6. Create unity of IO effect, despite disunity of command. Provincial reconstruction teams, the Department of State, government contractors, and civilian subject matter experts are just some organizations and enablers in the counterinsurgency battlespace. While such a multitude of organizations and funding sources often frustrate a military organization's propensity for "clean lines of command," the host nation population's perception is that all these entities are simply dysfunctional arms of the same force, the United States (or the coalition). Commanders must understand that creating unity of effect (as opposed to seeking unity of effort), even in the absence of unity of command, is essential because every organization's credibility depends on it.

Delegating IO resourcing and decision authority is critical because effective, local counterinsurgency solutions (and their IO components) look different to different localities. A company commander must have the authority to tailor IO messages, products, and staffs to complement the efforts of local, host nation, joint, and interagency partners with whom he must present a unified IO campaign in order to maintain credibility. Presenting the population with a unified national effect in counterinsurgency may paradoxically require delegating IO decision authority to as low a level as possible.

7. Ensure 24/7 staffing. Twenty-four hour IO staff coverage is necessary at every relevant echelon. We unintentionally build most IO cells to fail because most work 12-hour staff shifts without meaningful replacement for the remaining 50 percent of the fighting day. In the contemporary operating environment, insurgents and media "break" stories to the population within hours, yet counterinsurgent IO cycles often take days. Twelve-hour staff shifts and the consolidation of decision authority drive this tempo. Even when tactical leaders have the authority to conduct IO, staffs still have the responsibility to continually forecast, synchronize, and deliver assets to support tactical formations. Unless commanders resource and direct IO staffs to wage aggressive 24-hour operations with persistent coverage, within-minutes responsiveness, and IPB (intelligence preparation of the battlefield)-enabled precision in support of on-scene leaders who have employment authority, then the counterinsurgent delivery system is built to be unresponsive and irrelevant.

Models exist for the effective and responsible tactical employment of enablers—artillery, close air support, close combat air, medical evacuation. The employment of these functions is often dependent entirely on the judgment of tactical formations and leaders. The model is based on the need to provide tactical units with immediate lethal means to accomplish their missions because of the dire consequences for the tactical unit if we fail to do so. Recent counterinsurgency experience bears out that we must provide—with the same urgency with which we provide lethal enablers—instruments of nonlethal power like information operations, food aid, development expertise, and the Commander's Emergency Relief Program to tactical units in contact with the population and insurgents.

8. Plan and resource information operations into every phase of every operation. Every phase of the operation should incorporate IO, including possible branches or sequels.

Information operations' purposes and effects are roughly analogous to those of planning fires. They can—

- Enable the population's support of a patrol tasked to secure a road construction crew.
- Demonstrate the government's relevance and reach beyond its purely kinetic capabilities. For example, a planned press conference by the provincial governor next to a cache found by the host nation security forces during a deliberate operation, complete with a plan to insert and extract the governor and several members of the host nation media by air.
- Reinforce assertions of host nation partnership and relevance. (Enable the local police chief to announce the task and purpose of a nighttime air assault within five minutes of the operation beginning, even if the police chief himself only learned of the operation's details five minutes before that.

● Publicize a project's completion and each milestone in its progress. All school, road, and clinic openings should be reason for a press conference or social event sponsored by the host nation government (even if it is funded or enabled by the counterinsurgent coalition). In fact, an aggressive IO cell may hold a contractor-hosted luncheon to mark the approval of funding, a local power-broker-hosted press conference to mark a ground breaking, a "surprise" inspection by a government official (complete with media coverage), a provincial governor-led press conference and town-hall meeting upon the project's completion, and then ceremonies to mark as many anniversaries of the project's completions as are useful.[4]

An information operations battle drill should be in place in the event noncombatants are killed or property is damaged.

Planning for responsive, local IO—even when that operations' purpose is to mitigate the effects of a mistake—is essential to gaining and maintaining credibility. Deliberate operations planning includes a fires rehearsal, and it should include an IO rehearsal as well.

9. Build capacity and leverage local expertise. As with the pursuit of any goal in counterinsurgency, a coalition success without host nation partnership is failure. As counterinsurgents gain and maintain tactical IO dominance, they must train their host nation counterparts to do the same. The IO fight will last beyond the point that coalition counterinsurgent forces hand off exclusive responsibility to the host nation security force. Information operations' decisive role will not diminish with the transfer of responsibility, and the host nation force will require competent and aggressive IO warriors as much as it will need helicopter pilots, logisticians, and police.

Building host nation IO capacity also capitalizes on one of the host nation's strengths: host nation IO practitioners know the language, culture, and local themes and history that will enable IO to most effectively resonate with the population. Local information operations are most effective.

10. Seek feedback. Information operations are not fire and forget. Information operations are the successful *communication* of information or a message to a specific target audience. The broadcast of the information or a message is only the beginning of IO. The use of traditional and nontraditional media, face-to-face contact, interpreters, complaint procedures, hotlines, and provincial coordination centers to ensure that a message is received or to improve its dissemination is as important as executing the initial broadcast.

Dominating Information Operations

Despite the existing doctrinal gap and structural shortcomings, commanders at all levels must understand that dominating information operations is as necessary to success in counterinsurgency as dominating any other line of operation. If the counterinsurgent force does not dominate IO, then it cedes this potentially decisive tool to the insurgents. Because counterinsurgency's decisive point is the population, an IO system designed to enable responsive tactical effects to support tactical formations is essential. This effort will yield an enhanced ability to influence the population's perception of the host nation government as a preferable alternative to the insurgency.

Operational and strategic headquarters must actively facilitate their subordinate units' tactical capabilities to operate decisively along the IO line of operations by providing and resourcing constant staff support and a clear commander's intent in which subordinate units can exercise vigorous and disciplined initiative to achieve that intent. The lack of such clarity of purpose or priority of resources must not prevent tactical units from aggressively gaining and maintaining information operations superiority.

Tactical information operations are warrior tasks that fire teams, squads, platoons, companies, and battalions must execute with audacity to gain and maintain the IO initiative and wage relentless counterinsurgency operations. ***MR***

NOTES

1. Those that observe that public affairs and public relations are intentionally not part of information operations (IO) because they are independent disciplines miss the point: that they are separate disciplines is part of the problem. We must stop trying to make the tactical necessity fit the doctrinal definition and begin making the doctrine solve the actual problem.

2. LTC William B. Ostlund, *TF Rock Commander's Intent*, Operation Enduring Freedom (May 2007-August 2008).

3. Ibid.

4. LTC William B. Ostlund, CDR Larry LeGree, CDR Dan Dwyer, CPT Jeff Pickler, CPT Duane Mantle, and SFC Edward Hinojosa, *TTP's from TF Rock and Kunar PRT*, Operation Enduring Freedom (May 2007-August 2008).