# Shifting Fire:

Information Effects in Counterinsurgency & Stability Operations

### A WORKSHOP REPORT – ABRIDGED VERSION

CENTER FOR STRATEGIC LEADERSHIP U.S. ARMY WAR COLLEGE AND THE ADVANCED NETWORK RESEARCH GROUP, UNIVERSITY OF CAMBRIDGE



#### About the Workshop

The "Information Operations and Winning the Peace" workshop, held at the U.S. Army War College (USAWC), Carlisle Barracks, Pennsylvania, was a collaboration between the War College's Center for Strategic Leadership (CSL) and the Advanced Network Research Group, University of Cambridge (U.K.). It brought together, over a three-day period (29 November to 1 December), an audience of some 60 leaders and practitioners representing the military, national security, intelligence and interagency communities, as well as academia. It included representatives from the U.S., U.K. and Canada. Three case studies drawn from the Israeli-Palestinian conflict (second Intifada phase) served as the "driver" for small group analysis and discussion, and focused on the challenges of managing "information effects" in a counterinsurgency at the tactical, operational and strategic levels. The case studies provided a jumping off point for discussion of the issues and challenges facing U.S. and coalition militaries in adapting to the complexities of the "long war." The workshop was an unclassified event. The Israeli-Palestinian case studies allowed participants to engage issues without prejudice or risk to on-going operations.

#### About this Short Report

This short report is based on a longer workshop report, both of which were prepared by Deirdre Collings and Rafal Rohozinski of the Advanced Network Research Group, University of Cambridge, with substantive inputs from Dennis Murphy, Cindy Ayers, Dave Cammons and Jim White of the USAWC. Special thanks to Jim White and Bill Chanteleau (USAWC) for their support in providing transcripts of the workshop sessions and gathering research materials for both the workshop and this report. A word of thanks also to Brigadier General Vince Brooks (USA), Lieutenant General David W. Barno (USA) and Mr. Robert Petersen, U.S. Department of State, for their invaluable engagement with the workshop participants, which enriched the discussion and added greatly to the enthusiasm with which these difficult topics were debated. The longer version of this report – complete with the case study materials used in the workshop, the detailed takeaways, and an extensive bibliography – is available on line at: http://www.carlisle.army.mil/DIME/documents/Shifting%20Fire%20-%20Full%20Version.pdf.



# Shifting Fire (Abridged)



### **SHIFTING FIRE**

### Information Effects in Counterinsurgency and Stability Operations

A Workshop Report (Abridged Version)

By

**Deirdre Collings and Rafal Rohozinski** 

#### Shifting Fire

Information Effects in Counterinsurgency and Stability Operations

A Workshop Report (Abridged)

Executive Agent for the Workshop Report: United States Army War College

The views contained in this report are those expressed by workshop participants as captured by the report authors and do not necessarily reflect the official policy or position of the United States Army War College, the Department of Defense, or any other Department or Agency within the U.S. Government. This report is cleared for public release; distribution is unlimited.

Cover photograph by Sgt. Kevin Bromley, used by permission of the United States Army.

U.S. ARMY WAR COLLEGE CARLISLE BARRACKS, PENNSYLVANIA 17013

### Foreword

Information superiority is more than just the ability to muster superior information for the accurate and timely application of force. It is also the ability to compete in an increasingly complex and globally connected information environment wherein successful "textbook" tactical actions may risk serious strategic reverses or political "blowback." Senior Department of Defense (DOD) leadership was quick to recognize the importance of systematizing the military's approach to coordinating action in the information sphere. However, the process of adapting and employing this capability has proven neither easy, nor straightforward.

For decades, the U.S. military has been organized, resourced and trained to prevail in the physical realm. U.S. commanders are expert in the art of force-on-force engagement, but less adept at recognizing the links between kinetic action and the "information effects" they generate, and the impact this can have on the overall intent of U.S. strategy. Equally important, the military is still adapting to operating in an increasingly interconnected and integrated global media environment, where anyone armed with a hundred dollar digital camera and access to the Internet can become an "information warrior."

Adding to the complexity is the confusion of the modern battle space in which traditional state-based militaries have given way to an amorphous and ill-defined array of non-state actors ranging from local militias to networks of violent, ideologicallymotivated militants. In this rapidly evolving contemporary operating environment the U.S. finds itself fighting a global war on terrorism, while simultaneously pursuing counterinsurgency and security, stability and reconstruction operations in Afghanistan and Iraq. Even within a single theater U.S. forces are required to shift rapidly from combat to stability operations, or may find that both exist at the same time within a relatively compact geographic area; a condition which U.S. Army War College scholar Dr. Conrad Crane has dubbed "mosaic war."

As the U.S. military learns from its recent operational experiences, the necessity of thinking about "information effects" as both the intent and consequences of the deliberate use of force has come to the fore. If Information Operations (IO) is meant to accomplish a planned intent, then the concept of "information effects" compels a broader analytical lens that includes the *unintended* consequences of both IO and kinetic actions.

The U.S. and coalition militaries have rapidly moved towards an effects-based planning model for operations (incorporating IO as a major logical line of operations). However, anticipating informational effects that may be culturally specific, or dependent on a myriad of exogenous factors, continues to be challenging and raises a number of difficult and controversial questions. For example, how does one properly assess the potential for strategic blowback resulting from kinetic actions within the planning process, so as to avoid having the use of force become a liability to the broader aims of the global war on terror (and the all important "battle for ideas" on which victory is premised)? Is it possible to leverage IO to simultaneously compel and attract opponents and indigenous populations without the risk of message confusion or "information fratricide"? On a more fundamental level, is it possible to avoid becoming "effected" by your own strategic communication and IO in a globalized media environment? These are difficult questions without clear-cut answers.

Senior officers with experience in Afghanistan and Iraq have noted that existing doctrine is out of step with the reality of the field. Put bluntly: "There is no existing doctrine for the employment of the U.S. Army as an army of occupation tasked to establish a civilian government for a fractious and resistant population."<sup>1</sup> At a practical level, implementing the DOD vision of full spectrum "information dominance" remains ambitious and complex, leading to some confusion as concepts are applied in "real time" under conditions of "learning under fire." IO remains a collection of related and specialized practices. Some Army and Marine Corps leaders have expressed frustration with constantly changing definitions, and the fact that many of the IO capabilities exist at "echelons above reality" for troops operating at the

<sup>1.</sup> See Graff, J. K. (2004). "United States Counterinsurgency Doctrine and Implementation in Iraq." Command and General Staff College. Leavenworth, U.S. Army Command and General Staff College. Master of Military Art and Science: 87.

tactical level. There is also a tension inherent within IO and its constituent and associated competencies. Public Affairs Officers, in particular, have expressed concern that their core mission (to inform) is being interpolated with that of IO (to influence), which could lead to a "crisis of credibility" with the media and various publics. Some competencies, such as Electronic Warfare and Computer Network Attack are technically specialized and possess measures of effectiveness that are clear and quantifiable. Others, such as Psychological Operations, yield more subtle and difficultto-measure effects, which, according to a recent review of lessons learned, are often poorly understood by commanders who prefer to stick to more clearly measurable activities and outcomes (usually kinetic). An IO doctrine specific to stability operations in the midst of a counterinsurgency is also notably absent.

Many of these issues are being addressed as the U.S. learns from its experiences in Iraq and Afghanistan. But this comes with a cost as IO and "informational effects" are being experimented and implemented at the field level, and at the discretion of commanders. While this ad hoc approach can lead to rapid evolution and flexibility, it also creates problems for the continuity of effort, and at times, has led to the impression of incoherence, especially in the coordination of strategic messages.

The workshop on which this report is based occurred at an interesting historical juncture, just prior to the release of the updated IO doctrine, and draft Counterinsurgency doctrine, as well as the formal adoption of Security, Stability, Transition and Reconstruction Operations (SSTRO) as an accepted DOD transition mission. The insights and record of debate contained within this report reflect the tensions, frustrations and expectations among senior practitioners during a time of rapid change and mounting challenges. While the report captures important insights, it does not provide any clear-cut answers. Rather, it points to the complexity and scope of the challenges, and in this way provides elements of a roadmap for engagement.

The title adopted by this report – "Shifting Fire" – captures the essence of the task facing commanders and practitioners as they seek to understand and leverage information effects in an increasingly complex and networked world, where assessing the nature of threats and determining appropriate and proportional responses is increasingly difficult, and requires an interagency process at all levels.

Finally, the workshop and this report are the result of a unique international collaboration between the U.S. Army War College (Center for Strategic Leadership) and the Advanced Network Research Group (University of Cambridge). It demonstrates the vital importance of maintaining open channels among allies, and among the military, intelligence and academic communities as we collectively assess the challenge of collective global security. While perspectives differ, and conversations are sometimes heated and tough, it is through the spirit of engagement that a greater wisdom can be sought.

Rafal Rohozinski Advanced Network Research Group University of Cambridge

> Dennis Murphy Center for Strategic Leadership U.S. Army War College

### Contents

Foreword	V
Introduction	1
Twelve framing observations	5
Shifting fire: The changed battlespace	9
The challenge of response	13
Enduring challenges	21
Commander's concerns	23
List of boxes	
Box A. Informational effects: Summary of workshop takeaways from the Israeli-Palestinian case studies	3
Box B. The U.S. and insurgents view the war from different perspectives	8
Box C. The Stone and the ripples: U.S. versus insurgent view of the battlespace	Inside the back cover



#### Introduction

What are the boundaries and role of Information Operations (IO) when conducting counterinsurgency (COIN) in the midst of stability, security, transition and reconstruction operations (SSTRO)? What is the relationship between the political and military elements of the overall information strategy, and who is in charge? How do we counter indigenous insurgents without losing the hearts and minds of the population? If tactical actions can incur strategic informational effects (and losses), what responsibility does this place on the tactical commander? Do we have the right capabilities, amassed in the right way? These are some of the questions raised during the U.S. Army War College's December 2005 workshop on "Information Operations and Winning the Peace: Wielding the Information Element of Power in the Global War on Terrorism."

IO is (or at least should be) the main effort tactically, operationally and strategically in the current phase of the Global War on Terrorism (GWOT). At the global level, this effort is about winning the "war of ideas." At the theater level, the task is to combat asymmetrical adversaries, while establishing security, transforming the basis of government and extending the legitimacy of host nations. The central objective in COIN/SSTRO is to win the confidence and loyalty of "the people," so that they willingly support the host nation and your presence, rather than the insurgents. The central fight, therefore, is to establish the legitimacy and credibility of your agenda, your allies, and your actions in the eyes of the population, while discrediting those of the insurgents.

These new war-winning imperatives – to attract people rather than simply compel adversaries – greatly expand the role of information and perception management, which become primary aspects of the fight. From this perspective, IO needs to be considered beyond the doctrinal concept of five core capabilities aligned to influence opposing forces or shape the battlefield. Rather, everything that the military does and says in theater becomes a defacto information operation: all actions and words create informational effects in the perceptions of Tough questions about IO in COIN/SSTRO

> The "war of ideas" is informationled...

...and informational effects are key the population, whether intended or not. And beyond this, today's Global Information Environment (GIE) augments the complexity, by leveling the communication playing field, empowering the asymmetric adversary, and complicating the messaging picture due to the interconnectedness of different audiences and "real time" media reporting.

- Workshop design The workshop brought together an international group of some 60 IO practitioners from the military, national security and intelligence communities, as well as Middle East subject matter experts (SMEs). To spark debate, the workshop used mini-case studies drawn from the Israeli-Palestinian experience (the second Intifada phase) as a "jumping off" point for discussion of IO intentions and effects at the tactical, operational and strategic levels. The case study debates yielded 13 "takeaways" with general significance for thinking about the informational dimensions of power in COIN. (See Box A, on the next page, for summary; full takeaways are available in Appendix C of the long report.)
- Report focus But workshop discussions were not bound to the Israeli-Palestinian context; rather, participants built out from the Israeli-Palestinian context to raise issues and challenges related to informational effects that are facing the U.S. military and coalition members in current theaters of operation. U.S. military commanders are expert at conducting kinetic operations. They are less expert at recognizing the inseparable nexus between kinetic action, informational effects and the competition for influence of foreign audiences. Participants' exchanges on these issues form the basis for this summary, which covers the changed nature of the COIN/SSTRO battlespace, the challenge of effective response, and enduring challenges and dilemmas.

### Box A. Informational effects: Summary of workshop takeaways from the Israeli-Palestinian case studies\*\*

- 1. Never assume you are on the moral high ground, and that you therefore don't need to message. (Perceptions of moral authority/legitimacy)
- An intervening armed state tends to be seen as "Goliath," while nonstate actors that resist are often cast as "David." (Perceptions of moral authority/legitimacy)
- 3. Targeting insurgent leaders won't stop the resistance and the resulting informational effects may fuel further radicalization. (Tactics versus strategy)
- 4. Direct action against a threat may create positive informational effects with home audiences, but negative informational effects in the COIN theatre. (Informational effects: challenge of different audiences)
- When a campaign's strategic narrative contradicts the observed realities of your soldiers on the ground, it can hollow out the army's morale. (Informational effects: challenge of different audiences)
- 6. Eliminating insurgents won't stop the resistance or the terror tactics. (Tactics versus strategy)
- 7. When it comes to rumors of war-fighting gone wrong, the first stories onto the wire stick. Even if these stories prove to be exaggerated or false, the damage to your reputation, and moral legitimacy, is hard to erase. (Information sequel: perceptions of moral authority)
- Humanitarian action undertaken to limit civilian casualties should be documented and communicated before, during and after action. (Informational sequel and prequel: perceptions of legitimacy; preempting and dispelling rumors)
- 9. Even if you don't trust certain media, engage them. Restricting media gives an informational advantage to your adversary. (Information management: perceptions of legitimacy)
- 10. Western democracies have low tolerance for the moral ambiguities of kinetic action. This is especially so when, in the heat of battle, mistakes or civilian casualties occur. Kinetic action that violates the law of war creates informational effects that decrease domestic and Western support. (Informational effects: perceptions of legitimacy)
- Political messages that target domestic audiences can spillover to other audiences, and create detrimental informational effects in the COIN theater. (Informational effects: GIE and challenge of different audiences)
- 12. Cohesive all-of-government coordination can yield synchronization of the message, but not necessarily the effects. (Informational effects: Perceptions of legitimacy/perception management)
- 13. Information Operations need to keep going, even after the physical action is over. (Information sequel: perception management)

\*\* Takeaways are elaborated in Appendix C of the long report; case study materials are in Appendix B of the long report.



#### Winning the peace in COIN/SSTRO: Twelve framing observations

A synthesis of workshop discussions yielded 12 inter-related "framing observations" on "winning the peace" in COIN/SSTRO, which clustered around three key themes: the challenge of the new Global Information Environment (GIE); the changed nature of the battlespace; and, the challenges for mounting an effective, information-led response.

- 1. No single actor can control the information sphere. In today's wired world, the informational dimension of war-fighting has grown in importance, even as the ability to dominate the information sphere has decreased. New technologies, in particular the Internet, are readily accessible to a multitude of would-be "information producers," enabling almost anyone to conduct low-tech, yet sophisticated, "information operations" with a global reach. As one participant observed: "There are a lot in D.C. right now talking about 'information dominance.' I think we need to dispel that concept. You can't control or own the global information environment. We need to start thinking about how we plug information into that environment so that our information rises to the top."
- 2. In COIN, the center of gravity (COG) is the population, not the insurgent. An insurgency requires the support or acquiescence of the local population for all forms of intelligence and logistical support. This support is often readily given when the insurgency is native, and claiming to be "fighting for the people." A counterinsurgent will not prevail over an insurgency without winning the assistance, backing and trust of the local population.
- **3.** The primary objective is to attract and keep the people on your side. The fight is for the allegiance and trust of the indigenous population, and the "win" is achieved when the population supports you and the host nation rather than the insurgents. But this support must be given willingly if the objectives of stability and reconstruction are also to be achieved. (See Observations 9 and 10.)

GIE: A leveled playing field

Shifiting fire: The info-centric war

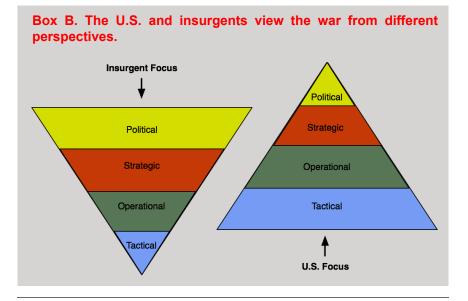
- 4. The main "fire" is informational: The task is to discredit the insurgent's strategy and means in the eyes of the population. Insurgents often have blood ties with the population you are trying to influence. Taking them out will not win "hearts and minds," but may well fuel future recruits. The "win" requires you to convince the people (and the insurgents where possible) that your way is the better way, and your ends are the better ends, which also requires discrediting the insurgent's ways and means. As a senior military commander underlined: "*The information element of power is primary; the focus is more on strategic effects than tactical combat.*"
- 5. The insurgent's advantage: They understand that the fight is for the lovalty and support of their people, and their principle "fires" are informational and political. That is how they are organized to fight. In the asymmetric war, insurgents cannot prevail using conventional means, and they do not try. Rather, insurgents use kinetic actions to achieve informational and political effects within the population, for example: to win adherents by undertaking daring physical acts to 'defend the people against the invading Goliath;' or, to terrify the supporters ('collaborators') of the liberating ('occupying') forces, and to undermine the peace and security promised by SSTRO. Moreover, insurgents capitalize on conventional kinetic actions undertaken by U.S. and other militaries by spinning the subsequent information effects to their own advantage, with stories of heroic martyrs or civilian casualties. Their ability to do this is enhanced because, often, military planners do not address sufficiently the informational "prequel" and "sequel" to kinetic actions, that is, to explain the rationale for action, to reassure the population, and to manage the after-action "informational effects." (See Box B on page 8.)
- 6. The U.S. disadvantage: IO continues to be focused more on supporting tactical physical wins, than on creating strategic informational effects. The U.S. administration and military are not yet organized or resourced to seriously fight the information-centric war in foreign lands. The U.S. channels wartime efforts and resources toward the tactical, physical level of war. As a senior military commander

stated: "We still see it as physically and kinetically centric, and we think about information as a supplement to that action. But in stability operations, your tactical work should be information-centric."

- 7. The military cannot go it alone: All dimensions of national power must be leveraged and coordinated in COIN/SSTRO. The informational effects perspective in COIN/SSTRO blurs the boundaries between the tactical and strategic levels of war, and requires the coordination of all dimensions of national power diplomatic, informational, military and economic (DIME). The melding of the tactical and strategic levels demands an integrated and coordinated information strategy across the military and political spectrum. As one participant noted: "We need to figure out how to choreograph this information picture instead of having a fight between our different communities about who transmits what at what time." (See Observation 8.)
- An effective and coordinated information strategy 8. defined strategic requires a clearly end-state, comprehensively understood. As one participant summarized: "The most important thing for developing an information strategy is to define what winning means. What does winning mean in Iraq? You have to start with that question." National policy and the information strategy flow from the answer to that question, with implications for what is communicated to domestic audiences, to allies, to opponents and to the foreign indigenous population.
- 9. The core challenge of COIN in SSTRO: To convince "the people" that your presence, agenda and local allies offer a more legitimate and credible future than do the insurgents. If you can get and keep the people on your side, you will win the peace. However, the very fact that an insurgency exists means that your legitimacy and credibility with certain groups is lacking.
- 10. The primacy of informational effects: Everything you do and say affects the people's perception of your legitimacy. Your legitimacy and credibility are based on how the indigenous population views your motives, your promises and whether or not those mesh with their own

The challenge of effective response needs and desires, and your delivery on those promises. This means that all your actions – from the theater level through to your soldiers' interactions with people on the street – and everything that you say, anywhere (in this GIE), create informational effects that either reinforce or damage your legitimacy and credibility in the eyes of the population. (See Observation 4.)

- 11. The imperative of message resonance: In COIN/SSTRO, "message dominance" is determined not by its pervasive presence, but by its resonance with the indigenous population. If your message doesn't make sense to the local population – addressing their hopes and fears, and expressed in their terms – it won't resonate. If it doesn't resonate, it won't stick.
- 12. The need for message consistency and coherence: All plans, actions and IO campaigns need to be considered from an overall strategic informational effects perspective, that is, their informational effects on the population's perceptual environment, and subsequent behaviors and allegiances. Messages (including actions) need to be consistent and coherent across all U.S. government actors, or information fratricide may result. (See Observations 7 and 8.)



#### Shifting fire: The changed battlespace

As noted, the core objectives for COIN/SSTRO are to: counter the insurgency, effect public security, extend the legitimacy of the host nation, and build towards a stable and self-functioning government. In this context, IO and informational effects are less about compelling adversaries or shaping the battlefield and more about countering an adversary while trying to win the allegiance and trust of the people who support or acquiesce to that adversary. These new imperatives have important implications for how one understands the COIN/SSTRO battlespace, and the unconventional ways and means that are required. Workshop discussions clustered around four key themes:

### 1. Kinetic action to counter insurgents can create negative informational effects

Participant's accepted that the policy of targeting insurgents for physical destruction is based on a belief that such action will eliminate known trouble-makers, deter future recruits, and thereby effect security, a primary requisite for SSTRO. However, discussion of the Israeli-Palestinian case studies revealed that a mostly kinetic approach to hunting down Palestinian targets appears to have further fueled and radicalized the resistance movements, rather than stamping them out. Moreover, with respect to SSTRO objectives, a kinetic-heavy approach can cause added complications due to:

- Blood and communal ties. Indigenous insurgents are usually tightly networked into the population. A strategy that seeks to portray the insurgent as undesirable is unlikely to resonate very widely with "the people." Moreover, once a cycle of killing starts, "blood feuds," revenge killings and other traditional systems of honor can perpetuate and widen popular support for the insurgency, quite independent of its original sources.
- Shared grievances. An insurgent who claims to represent communal or national grievances may well command a legitimate popular following. If those grievances remain

Taking out insurgents...

...can fuel new recruits

unaddressed, taking out the insurgent will not end the resistance. Rather, a kinetic approach can strengthen and radicalize resistance movements, while drawing the "resistance" closer to the population.

- Future political partners: Today's insurgent may be tomorrow's political ally. Labeling certain groups or individuals as "terrorist" and irredeemably "evil" can close down future opportunities for political engagement and settlement. Terrorism is a tactic, not an immutable trait.
- The need to reinforce the rule of law as the basis for dispute resolution within society. An SME, reflecting on the Israeli COIN approach of "targeted killing" and administrative detention of terrorist and insurgent suspects without trial or evidence, noted that such tactics do not reinforce faith in the systems and institutions of justice and law within Palestinian society. Extending this argument, participants concurred that from an SSTRO perspective, reinforcing security through the re-establishment and strengthening of the "rule of law" and its attendant institutions is a critical priority. An international participant commented that the present-day U.S. situation, where the ROE remain oriented to the priorities of major combat operations, may warrant a rethink given SSTRO's "rule of law" objectives.

### 2. The new importance of informational "fire": Discrediting the insurgent's strategy and actions

So, it is better to discredit their means A senior military commander observed that a central focus in COIN is to discredit the insurgent's strategy and actions, and that this fight was information-led: *"Tactical action is really about convincing the indigenous citizenry that the insurgent's strategy and actions are discredited...It is about gathering information and evidence to fight the informational fight for the hearts and minds of the population...The information component is primary, not secondary." However, the information campaign must be based on why <i>the population* might think insurgent actions are illegitimate, and not on why *you* think these actions are illegitimate. That is, the campaign must work to challenge

...and may also eliminate potential future allies. the legitimacy and credibility of what the insurgent says he is doing in the eyes of the population, and in a way that resonates with local cultural and resistance narratives. This requires deep cultural capacity, and close understanding of "what is sensitive to the adversary." As a senior commander noted: "Documenting what the enemy is doing [when it stands in contradiction to what he says he is doing] becomes powerful ammunition in this information war....Your intelligence collection plan for imagery, for example, is not to find the best avenue of approach, but to document evidence that the fighter is hiding behind women [when he fires]."

#### 3. The new importance of addressing motivations

Workshop debates on how to end an indigenous insurgency (with a popular or acquiescent following) kept coming back to the issue of motivations, which kicks the problem up to the political and interagency level. However, the discussions threw up five roles for the military in addressing "motivations," given that it is the force on the ground in COIN/SSTRO:

- To ensure the safety and security of the population, which can help to win over those who acquiesce to the insurgency out of fear, or whose support for insurgent methods is wavering. However, this is a tall order, given that insurgents engage in kinetic action for the residual informational effects of creating insecurity, and keeping any potential dissenters in line. As a senior commander noted: "The degree of threat on lives [made by insurgents] can be a much more compelling argument than the one that we will make...We can try to convince them that their lives will benefit if they work with us. But at what point is someone willing to expose themselves and their family? This is a very complex dynamic."
- To document evidence that discredits the insurgent's strategy and actions in the eyes of the local population.
- To ensure own soldier actions do not alienate the population and/or increase their motivation to support the insurgents. Soldiers are the main point of contact with the population, and their behavior – good or bad, respectful or humiliating

Document your adversary's hypocrisy...

> ...and work to cut off the stream of motivation

> The military has a role to play...

– exerts enormous effect on the population's understanding of what your true intentions must be ("you are here to help me" or "you are here to humiliate and conquer").

- To have the "hammer in reserve." One participant noted that the "hammer" must be leveraged for its informational effects: "If everyone knows you've got the hammer in reserve, it is important that when a situation happens you deal with it in a mature manner so you are not dropping that hammer every time a minor offense occurs. And in that way, you may build a little more credibility with the people you are trying to reach. It's a pebble at a time; an incremental process."
- To play a role in keeping the channels of communication open. As the on-the-ground presence, the military can play a role in keeping the channels of communication open with the insurgents and population that supports them – not for negotiation (which is obviously not the military's preserve), but as a channel for dialogue and signaling.

### 4. The need to leverage all aspects of national power – DIME

Participants recognized that strategic informational effects ...but DIME is what is needed encompass all lines of U.S. government (USG) power diplomatic, information, military and economic (DIME): "It is no longer a matter of exercising a military option with IO in support of it. To look at it just from the military perspective is difficult to do, even in a DOD IO sense, because IO has to be integrated with the CMO plan, and the other elements." Participants concurred that "we should all work together," but recognized that strong organizational challenges remain. Participants agreed that the military needs clear strategic guidance on the proposed endstate and overall information strategy to effectively fight the informational fight. However, this strategic vision sometimes has been lacking, which has meant that, by default, the military was shaping policy through its actions on the ground. Many also thought that overall coordination mechanisms are lacking. and wondered who is in charge of the overall IO effort in DIME. (See "Enduring challenges," page 21.)

## The challenge of response: The battle for legitimacy

Ultimately, the war for "hearts and minds" is a battle for perceived legitimacy and credibility in the eyes of the population – that is, the legitimacy and credibility of the intervening power and host nation versus that of the insurgents. The workshop spawned significant discussions on the role of information and cumulative informational effects in this fight. Participants concurred on the criticality of message resonance. To be effective, a message must "resonate" with the hopes and fears of the population, be expressed in terms they understand, and be consistent across all allied actors in terms of both words and actions. To date, this has proven challenging, as different participants observed:

"One of the problems we've had with U.S. PSYOP messages and propaganda is that nobody listens to them. They blow them off. We come up with new newspapers, magazines, TV stations, but if it's got the U.S. flag on it, it gets pushed aside."

"We talk about fighting a war for hearts and minds, but... we have really only been appealing to minds. We say: 'This is why you want to be Democratic. This is why the Western way is the way to go, one person, one vote.' We lay out a good argument, but the insurgents don't bother with any of that crap. They understand what motivates the people emotionally. You can make the best argument in the world, but they've got that Mom-and-Apple-Pie-Shaeed (martyr) thing going, and that reaches the people's hearts. So they can get people to do seemingly irrational things because of the emotional response. They know how to motivate symbolically, emotionally, and at their very core. We've been fighting the mind side, while they've been fighting the heart side ... and guess what? They're winning." ...and message resonance is key

The battle is for

legitimacy...

Discussions about the challenges of message resonance clustered around three inter-related issues:

### 1. The challenge of legitimacy (1): How you are perceived

Messages must account for how "they" see "us" Understanding how you are perceived by the target population is a critical building block for designing appropriate informational "shaping" effects: "We may not consider ourselves to be occupiers, but that doesn't answer the political question that the audience we have to influence may see us as imperialists. Unless we factor in how they see us, we are wasting our time." Participants raised four elements that can shape baseline perceptions of U.S. legitimacy in the eyes of the foreign population:

- Residual informational effects of past historical actions, which form an "informational prequel" against which your intentions and actions will be assessed. For the U.S. in Iraq, the residual informational effects of past policies and action in the region are particularly important. As a senior military commander noted, "[How we are perceived] is not something that starts with a decision by us to engage." Participants concurred that the different turns in U.S. policy in Iraq since the 1970s have likely contributed to the mistrust of current U.S. intentions.
- Residual informational effects from regional friendships: The mistrust of U.S. intentions. Many participants concurred that America's strong support for Israel, as well as certain authoritarian Arab regimes, negatively influences the perceptions of U.S. intentions at the popular level in the Arab and Islamic worlds, and makes the U.S.' fight for trust and credibility with those audiences more difficult.
- Inadvertent hubris: Assuming you are on the moral high ground. No matter how much you believe in the rightness of what you are doing, you should never assume you are on the moral high ground. One participant, sharing the views from a conference that brought together foreign Defense Attachés, stated: *"There is a real sense that both American messaging*"

*and policy project cultural hubris.*" Much work is needed to discern where the moral high ground lies in the eyes of the population, and to craft policies and information strategies that resonate with that terrain. But this process is not about simply adjusting the words so they sound right. Rather, it is mostly about backing a policy that is seen to be legitimate.

• When your actions contradict the values you profess: The "Goliath Syndrome." Participants noted that a "David and Goliath" syndrome seems to color most encounters between armed state actors and non-state "resistance" actors who claim to represent a cause. This is particularly true when the U.S. is involved, both because of its superpower status, and its stated purpose to uphold and spread freedom and democracy. Such a value-laden agenda brings high moral expectations: "The rest of the world expects our country to act from the moral high ground. Our ability to act effectively – even among those who may not like us – has always depended upon the sense that what we did respected the dignity and worth of human beings and of freedom. If you lose sight of that in your information strategy, you might as well go home." In other words, if your actions contravene the values you claim to represent, this hollows out your legitimacy and credibility, and the "war of ideas" will be lost

### 2. The challenge of legitimacy (2): Crafting messages that resonate

A critical indicator of effective message resonance is "reverberation," that is when members of the population pick up the message and repeat it to secondary and tertiary audiences. Discussions centered on two critical capabilities for creating messages that resonate:

• Cultural capability: Not yet sufficient. Participants concurred that COIN/SSTRO information objectives require deep cultural knowledge. The military's need for cultural capability has expanded considerably since 2002, but its actual capacities have not yet caught up: "The Army PSYOP force has people that have lived in the region, or come from those cultures and know the language and

Messages must make sense to them religion. However, your 21 year-old farm boy from Iowa doesn't know about these things. And the scary part is that a lot of other IO practitioners don't understand these things. So they "mirror image." They use a U.S. perspective and then are puzzled when it doesn't work. Why are we creating another generation of terrorists? That is what happens if you don't understand the motivations."

Situational capability: The need for local knowledge on a war-time footing. Beyond "cultural capability," what is also needed is fine-grained, locale-specific situational knowledge of the local social networks, power relations, and issue clusters, which can be very different from and yet interact with those in other locales and regions, and which can also evolve rapidly in an on-going conflict situation. Building this situational capability requires intensive time and engagement on the ground. Some participants thought that the U.S. still doesn't understand that "IO or PSYOP are not short-term weapons systems. You have to establish and build credibility over years. Any IO solution has got to be built up over time: there is no quick fix."

### 3. The challenge of credibility: Message delivery and coherence

Credibility is measured by the degree to which you are trusted and believed. Without credibility, there can be no legitimacy. Participants discussed six elements that can enhance message credibility:

A respected local spokesperson is best

- Use local messengers with good social capital. A respected member of the target audience is by far a superior conduit for moving a message than a U.S. spokesperson or designate.
- Use local media, including those you consider to be "hostile." A number of participants stressed the need for the U.S. to engage al-Jazeera "every chance we get," because of its credibility and influence with the target audience.

- Ensure message continuity: The information sequel to physical acts. As noted, U.S. commanders are expert at conducting kinetic operations, but less expert at anticipating the "informational sequel" to these actions. Insurgents have readily filled this "information gap" by negatively "spinning" U.S. actions in the minds of the population, which can undermine the physical success of an operation and hand the insurgents a strategic win. The instantaneous interconnectedness of the GIE places a heavy priority on pre-operation planning to prepare the informational battlespace, and preempt damaging disinformation. It is critical to document and advertise what you do, especially the humanitarian efforts and own force risks that are taken to protect civilian lives. However, participants noted that, currently, information management efforts can still be deprioritized by tactical tradeoffs. This problem has arisen in both Afghanistan and Iraq on occasion, when trying to bring in combat camera: "We couldn't get them butt space on a helicopter because the tactical commander decided he needed more guns, and he didn't need a guv running around with a camera." These kinds of decisions, the participant continued, are made independently of the bigger picture and the message that needs to get out, "especially in the case where things go wrong, which they quite often do."
- Actions and Words (1): Soldiers are your "informational" frontline. Message credibility can be reinforced or eviscerated by soldier actions on the ground. What soldiers do – how they approach people, how they behave during a confrontation, how they are outfitted – form the "real experience" that the people use to judge the credibility of your intentions. Do the people feel you are there to protect them, or to protect yourself? It takes a very long time to build up trust with the population, and only a moment to destroy. Troops at the lowest levels need to understand that their behavior creates an "information effect" with potential strategic repercussions. Beyond this, overall force posture also carries an important message to the people. Some participants thought the U.S. was missing an opportunity here: "*Apparently our troops are pretty much required to be kevlared up*

...and the messaging needs to keep going

Every action has an informational effect... at all times, and that often sends the wrong message. British commanders have greater latitude, and can use that to send different messages..."

Actions and Words (2): Deliver the goods. Credibility requires that you are seen to "deliver the goods, not just sell the goods." If you or your government are promising things that you can't deliver, or that the local population does not value, your credibility and capacity to influence are lost. Failure to deliver is fuel for insurgent recruits, as a senior commander observed: "You said that my life was going to change for the better. But my life has changed not a bit. I can prove for myself from my experience that your message is false. So I think you are a liar. And so did my father. So I'm going to seek to kill you, because I know you will do nothing for my son."

• Maintain credibility across different audiences: The troubled relationship between IO and Public Affairs. Participants debated the difficulty of maintaining the consistency and credibility of message content across different target audiences, and of de-conflicting and synchronizing IO and Public Affairs (PA) given the new interconnectedness of the GIE:

Mosaic audiences pose messaging conundrums... - Message consistency across different "in theater" intentions and operations. The COIN/SSTRO theater presents inter-connected local audiences, some of whom you want to compel and some of whom you want to attract. From an information effects perspective, problems arise because OPSEC, MILDEC and PSYOP are often used to shape operations against insurgents in ways that can, at times, conflict with the broader imperative for building confidence and trust among the local population. This is particularly the case under conditions of a "mosaic war," where the intensity of combat operations and reconstruction efforts may vary greatly between adjoining districts, or even within a single district; where shifts between stability-oriented versus combat-oriented messaging can happen rapidly; and, where different potentially U.S.-friendly audiences may not like or trust each other. Many participants argued that such a complex information environment requires being as accurate and transparent about explaining your intentions and actions as OPSEC permits. As one participant opined: "When it comes to building and keeping allies, the foundation of a PA campaign, but also Information Operations, is truth. Truth is not malleable. When it is manipulated, vou lose all credibility... As a political consultant, I can tell you that the first thing we look for in any campaign against our numerous adversaries is a misstatement of truth. It doesn't take much to destroy the credibility of an information strategy. The United States, as a white horse, means one black speck shows up very clearly. This is not true for our adversaries. It's just a burden and a political reality that we need to deal with." While accepting this logic of transparency and truth, some participants wondered at its practical feasibility.

- Foreign and domestic audiences in the GIE: No more "iron fence." The GIE - where just about anyone can become an information producer with global reach, and where the distinctions between foreign and domestic media are blurred - has made it difficult, if not impossible, to retain an "iron fence" between IO and PA, that is to ensure the integrity of U.S. information that finds its way to U.S. domestic audiences. Participants concurred that IO is premised on influencing and shaping perceptions, which can result in messages that are, while truthful, "spun" to meet this premise. This lack of full transparency in messaging calls into question the dividing line between truth and deception, which is the crux of the friction between PA and IO.<sup>1</sup> While some participants argued that a clear distinction between IO and PA must be upheld, many participants also accepted ...and information knows no borders

19

IO and PA are legally separate...

<sup>1.</sup> The loose use of the term "IO," even by practitioners, may in fact exacerbate this problem. IO includes both the capabilities of military deception (meant to deceive the adversary as to friendly operational intentions) and psychological operations (meant to influence perceptions based on credible messaging). "Messaging" here refers to psychological operations.

the inevitability of "message spillover," as the following workshop exchange illustrates:

	<b>Speaker 1:</b> Information Operations is conducted against your potential adversaries, decision-makers and decision- making processes. Do we always tell the truth? No. But we cannot deceive the public. There should be a dividing line here between home audiences whom we don't do PSYOP against – whom we don't deceive or try to "influence. Media Operations or PA that is a separate issue.
but are they in practice?	<b>Speaker 2:</b> Are they really separate? I mean from today's information environmentin a practical sense. Are they really separate?
	<b>Speaker 3:</b> They are legally separate but in practice they are not. Something we tell a local audience at a Rotary Club meeting can have global exposure depending on who takes that message out.
	<b>Speaker 4:</b> Yes. For example, General X made a casual statement about religion, which was broadcast globally by text messaging on a cell phone that same day. It goes back to your point about living in a global 24/7 environment.
Talk of - "crusades" just won't do	<b>Domestic commentary creating informational effects</b> <i>in the foreign battlespace.</i> Given the GIE, domestic political rhetoric is also an informational fire (or misfire) in the fight for foreign credibility and trust, and must be treated as such. Some participants argued that the use of the term "crusades" in U.S. domestic speeches in the run-up to the war in Iraq was likely unhelpful for setting the right perceptual environment with the Iraqis, no matter how well this image may have played at home. Another participant observed that the term "axis of evil," developed for domestic political consumption, has had major implications for U.S. foreign policy. A number of participants concurred that the military – as the front line that faces the perceptual environment of the population – needs to be fully aware of how their mission is being framed in domestic pronouncements at all levels.

#### Enduring challenges: The big picture

Participants broadly concurred about what "should" be done to prevail in COIN/SSTRO, but thought that the "shoulds" are out-of-step with current capabilities and organization. Rapidly evolving events and in-field learning have been outpacing the military's ability to fundamentally transform itself at the overall institutional level, with negative knock-on effects in the field. In big picture (organizational) terms, participants discussed five key challenges:

**Institutionally and culturally, the priority is still on kinetic war-fighting skills.** This is where the money and training goes. (See Box B on page 8.)

Force turnover timeframes are too short for effective **IO.** Effective IO requires "time on the ground" to attain the necessary cultural and situational capabilities, and to gain the trust of the people. At the same time, force turnover is necessary. Experience has shown that force turnover can sometimes incur a strategic setback due to differences in force posture, training and approach: "In Afghanistan, we had Special Operations Forces working in a village for the better part of a year. They were very culturally attuned, spoke the language, and did not come in with heavy guns. They were replaced by a unit [of the] airborne division that came in full flack jackets, up-armored, very by-the-book tactical military force. And within two weeks they totally undid all the good will that the Special Operations Forces had built up over a year. They were different types of units, different visions, with different training. So not only did we have the timeframe, the rotational aspect, but we also had the different types of units. This is a huge deal, I think, for what we're talking about."

How do we achieve information cohesion across agencies and levels, and who is in charge? Clear strategic policy guidance is not always present, or present at all levels. Without such guidance, individual commanders are left to interpret and construct messages based on their own understandings of their particular locales – with predictable negative consequences

We understand what "should" be done...

...but the required support system is lagging behind...

> ...as is the coordination: Who is in charge?

for the overall coherence and continuity of effort, especially in a mosaic war. Participants expressed three concerns:

- *Top down: Who is responsible for overall "message cohesion?"* Participants concurred that responsibility for strategic message cohesion lay with the interagency level, but were concerned that an effective, coordinating DIME edifice was not yet in place. There were many questions about how all the USG pieces are meant to fit together: Who is in charge of defining the overall information strategy? Who is in charge of message coherence and discipline at the strategic level? How does that strategic vision make its way down to the tactical commander's level?
- Bottom up: Who is empowered to adjust "informational fire" to ensure message relevance? A senior military commander emphasized that while message discipline is essential, messages must also be relevant: "If the message is not the right message, then discipline and compliance are not the order of the day. Revision is the order of the day." This need for flexibility and responsiveness suggests that local ad hoc adaptation is critical. At the same time, however, overall message coherence across different audiences/locales suggests the need for higher-order guidance. This dilemma remains unresolved.
- *How do we prevent "information fratricide?*" Given the top-down, bottom-up conundrums, many participants were concerned about the potential for "information fratricide" in the SSTRO environment. Some argued that a new governmental body was needed to give greater coherence to the informational dimensions of an all-USG effort.<sup>2</sup> Others, however, with a nod to past failed attempts at improved coordination, wondered whether this degree of inter-departmental "communication fusion" was likely anytime soon.

<sup>2.</sup> Note: Karen Hughes was sworn in as Undersecretary of State for Public Diplomacy two months prior to the workshop. The impact of this new interagency office was not yet evident to most participants.

Can we expect to reach all critical audiences all the time, without sending mixed messages? Given the diversity of audiences, narratives and viewpoints, some of which may be in open conflict with one another, participants wondered whether it was possible to ensure overall message consistency and whether USG capabilities and coordination were up to the challenge. As one participant emphasized: "To me, this is the crux of the current IO conundrum: How do you tailor and convey messages to different and often contradictory audiences in today's information environment?"

What is the emergent relationship between IO and PA in COIN/SSTRO/GIE? While IO is meant to "shape" and PA to "inform," the GIE has eradicated the guarantee of an "iron fence" between the two, and may compel new levels of transparency in foreign theaters. As one participant observed: "The central challenge for 'truth' within the COIN/SSTRO environment is the interconnectedness of the audiences you are trying to compel, to attract and to inform." Many participants were looking for guidance on how to handle these fundamental challenges: "PA doesn't want IO in charge. And PA says we can't have IO working for us. Who is responsible for pulling this process together?"

#### **Commander's concerns**

In today's rapidly evolving COIN/SSTRO environments, "*the commander is his own IO [planner]*," meaning he needs to understand how to wage an information-led war and consider all undertakings from an informational effects perspective. Many participants thought that commanders are not receiving sufficient guidance, authority or capabilities in the manner needed to carry out their expanded, information-centric duties. Concerns were voiced across ten issues:

**Operating without clear policy guidance.** If a commander's operations may incur second and third order informational effects, then he needs a clear understanding of the overall strategic endgame, and the strategic consequences of dealing with "*that particular bad guy in this particular way*." But this

This new way of war-fighting expects much of commanders...

A key IO

conundrum...

...with doctrinal implications framework has not always been in place: "Most combatant commanders are struggling with exactly what the national policy is. In many cases they will come up with guidance even if none is formally given. And if actions are spontaneous, there may not be an IO plan in place..." In the absence of strategic guidance, commanders may create "strategic policy de facto, through our tactical and operational events," which in turn may created unintended political effects. This, some argued, "may not be the best thing for the government and everyone else involved."

...and is blurring the boundaries of our responsibilities.

How all-seeing is the commander expected to be? Are higher order informational effects of tactical actions the commander's responsibility? The new melding of the tactical and strategic levels of war in COIN/SSTRO (from an informational effects perspective) raises many questions about the limits of the commander's writ. Some participants were adamant that a tactical commander's job is to follow orders. But others disagreed: "If we assume that consideration of informational effects is now an essential part of the planning process for any tactical engagement, it doesn't make sense to choose a deliberate engagement in a symbolic-laden spot like the Jenin refugee camp.<sup>3</sup> If your objective is to defeat the motivation for terrorism, choosing a showdown in Jenin is more akin to a recruiting tactic. In COIN, a target cannot be chosen for purely tactical military purposes." Participants concurred that commanders need to be empowered with the understanding that they have a wide menu of different tactical choices, so they do not feel compelled to default to the most kinetically expedient. But the complex questions about responsibility for higher order effects remained.

Limited capabilities compromise results... We are not confident that we have sufficient strategic vision and capability at the brigade level and below to make the right choices. Participants were concerned that the overall strategic vision and information strategy were not making it down to the tactical level, and that on-the-ground capabilities were not sufficient for making sound strategic choices:

<sup>3.</sup> Participant is referring to the Jenin case study. Other participants drew a parallel with Fallujah in Iraq.

I am very good at putting little red dots on people's programs and telling them we're going to do this. But if I don't understand the bigger aspects, then I am not going to have that comprehensive view at the tactical level, and I'm going to continue to win the battle and lose the war. So I need diplomacy. I need somebody who understands the second or third order effects of me going in and doing these things. How do I get that vision to the tactical level? You tell me, I don't know.

You have to make choices... But you have to truly understand the culture that you're operating in. And that is a challenge for a brigade, a division or a corps because they don't necessarily have access to the appropriate level of detail.

If I see an information liability or opportunity, do I exercise my own initiative, or should I check back up the chain of command to ensure no unintended second or third order strategic effects? Does that feedback loop exist? The commander is well placed to see when the policy from above is out-of-step with the ground truth. But, some participants wondered what channels exist to provide feedback up the chain of command if, from a ground perspective a given task may risk wider strategic blowback, or if new opportunities were arising:

The policymakers might ask the military to try to achieve some ends that are not reasonable. In my previous experience, we could actually go back and say, 'This doesn't make sense. It's not doable. We may get to Point B, but that doesn't achieve our stated ends.' But this has been one of the areas that has been troubling me, personally, for the last four years.

As the subordinate IO and PA officers, who do we go to when we see an opportunity at the tactical level for a strategic benefit? So that we can reinforce the message or change the message to be more agile, based on something that is happening in my area of operations? ...and coordinating mechanisms are not clear...

## ...while the complexity is fierce

The complexity of the mosaic battlespace: How do we aggregate complexity back up the chain of command? Situational complexity in a mosaic war presents huge challenges for message coherence and effective IO, especially given present capabilities. Different locales can be very diverse, and for the IO officer, understanding the complexity of each local environment, and then aggregating this up to the next level so that a commander can understand the overall IO picture is hugely challenging: "*The complexity a sergeant* or a lieutenant sees on the ground is difficult to convey up to staff officers, who must reallocate resources in a flexible and agile way, as an insurgent in a local area can do. And that is something that the commander has to account for in his risk factor. It requires extensive coordination – up, down, right and left – to make sure you understand what you are doing."

Is there sufficient capability to sustain agile, 24/7 IO at lower tactical levels? Some participants expressed concern about the "lack of density" of IO staff at the more junior levels of the command structure, which compromises capacity for providing the all-seeing, 24 hour at-the-ready stance that is seemingly expected at the tactical level. Using the example of responding effectively to rumors, a participant noted: "*We don't have sufficient clarity of information for the people who have to put the response message together, to "return the fire." Nor do we have the organizational process in place to ensure that we have that clarity. We leave it up to a lot of people who are doing their best. But the lower levels are greatly challenged by the variety of tasks that they are now responsible for.*"

Is there sufficient cultural capability at the tactical level? Most participants thought the military was lacking in cultural capability overall, and especially down at the ground level where it really counts.

When security requirements contradict the overall strategic messaging about our objectives in the eyes of the population, what can a commander do? A tactical commander and his soldiers face the people on the street. But, asked one participant, what happens when U.S. strategic messaging doesn't agree with what people see and experience: *"For instance, the U.S. says, 'we are here to help establish this and reestablish that.' But what the people see you doing is going around clearing out houses, searching ambulances, patting women down at checkpoints, and stuff like that."* Everybody acknowledged that the insurgents are well placed to spin the informational effects of such action in a way that resonates with the people's experience: *"The insurgents are saying that is because you are disrespecting them or you are trying to hurt them."* But participants were at a loss as to how to conduct necessary security measures in a way that did not alienate the population.

Bringing the boys back home. In the mixed COIN/SSTRO environment, do you take own force risks to "send the right message" (we are there to help and protect you) to the population? From a trust-building perspective, soft hats and respectful, low-key behavior at checkpoints should be the order of the day. But is that realistic to expect in a COIN environment? Some participants with recent field experience thought not: "[The commander] has objectives, and he is going to accomplish them, but he wants to keep as many of his troops as safe as possible. Is he thinking about the long-term? *Is he thinking: 'Five years from now, how is the teenage boy* that we're roughing up going to behave? Are we going to turn him into a terrorist?' No, he is not thinking long-term. He is thinking about achieving the tactical objectives and keeping the troops safe to bring them home... He doesn't care what happens 14 months after he is gone."

Accepting casualties for IO effects? A senior military commander, stressing the need to be thinking about combat operations for the sake of pursuing information value, asked: "Are you willing to put someone's life at risk in terms of selecting a mission that will involve physical risk, perhaps the loss of life, for the sake of information? That may sound heretical for a General to say, but I submit to you that the absence of such a view is what often leads us to miss opportunities." On a related front, discussion of the Can security measures be conducted *without* alienating the people?

And whose safety comes first?

Do we risk soldiers for informational effects? Jenin case study illuminated what can happen after own force losses: force protection takes priority, ROE may break down, and excess civilian casualties result. For the Israelis, the result was an information debacle with stiff strategic consequences. Participants concurred that this dynamic occurs all the time: "When you take enough casualties, it changes your view about what is ethical and the scope of tactics that are acceptable. And that has a profound impact on the IO strategy itself." The harsh response sends the message that your own protection is more important than the protection of the local population, which incurs a strategic informational loss. The best that can be done after the fact is damage control, although rational explanations of why civilian deaths occurred are unlikely to have much resonance. Participants emphasized that from a strategic informational effects perspective, own force restraint is absolutely critical. But is that realistic to expect of your soldiers or your commanders in high-risk situations?



### Box C. The stone and the ripples: U.S. versus insurgent view of the battlespace

Participants concurred that although the U.S. military has been rapidly adapting to the information-centric battlespace, its organization and training are still weighted towards conducting physical action to achieve the desired effects. By contrast, insurgents conduct physical action mostly to achieve strategic informational effects. Borrowing and building on the "stone in a lake" metaphor developed by Emery et al. (2005),\*\* we can see the relationship as follows: When you throw a stone into a lake, that physical action causes ripples across the water; the ripples are the residual informational effects of the physical act. As Emery argues, "long after the stone has hit bottom, the residual effects of the act carry on in all directions and are difficult to interdict, ultimately crashing into the banks of the lake."

**U.S.: focus on the stone.** As Emery notes: "The current non-state conflict strategy focuses on the splash of the stone – the physical effects – and not enough on affecting the ripple – the informational effects – before it reaches the bank." That is, before it has an impact on the perceptions of the population. The U.S. military tends to be focused on the stone.



Insurgent



**Insurgents: focus on the ripples.** By contrast, insurgents use physical action to leverage the informational effects – be that to attract recruits through the "bravery" of their actions, or to spread a sense of fear and insecurity within the population. The insurgent focus is the informational ripples, not the stone.

**Insurgents also leverage the ripples of the U.S. stone**. Insurgents also seek to leverage the informational effects of U.S. kinetic actions. When the U.S. throws a stone, the insurgents are busy spinning the informational ripples – "see the civilians killed by the occupier?" The insurgent's spin is more powerful when there is no counter-message, that is, when the U.S. ignores the informational sequel to its physical acts.



\*\* Reference: Emery, N., Mowles Jr, D.G., and Werchan, J. (2005) Information Operations Doctrine and Non-state Conflict: Shaping the Information Environment to Fight Terrorism and Insurgencies. IO Sphere. Spring: 5-11.