Global Tides

Volume 1

Article 3

2007

# Influence in an Age of Terror: A Framework of Response to Islamist Influence Operations

John Deniston
*Pepperdine University*

## Recommended Citation

Deniston, John (2007) "Influence in an Age of Terror: A Framework of Response to Islamist Influence Operations," *Global Tides*: Vol. 1, Article 3.
Available at: https://digitalcommons.pepperdine.edu/globaltides/vol1/iss1/3

Running Head: INFLUENCE IN AN AGE OF TERROR

# INFLUENCE IN AN AGE OF TERROR:

## *A Framework of Response to Islamist Influence Operations*

John Deniston

Pepperdine University

## ABSTRACT

Adversarial influence operations perpetrated by Islamist terrorist networks confront the most foundational of America's national defense capabilities: the will of the American people to fight. This assertion is predicated on four key determinations. First, Islamist terrorist networks use influence operations as an integral tool of global jihad. Second, these adversarial influence operations should be perceived as attacks and, subsequently, should demand response. Third, a wide array of US Government tools and institutions currently exists to counter this challenge. Fourth, precision-strike doctrine and cyber-attack response frameworks provide instructional examples of methods to create a coordinated US Government response to such influence attacks.

This analysis seeks to bring two new contributions to the counter-influence policy dialogue. First, based on the determination that influence attacks are legitimate matters of national security, this paper recommends response to these events be viewed through the prism of existing military doctrine. Specifically, the same precision-strike doctrine used to neutralize threats with kinetic means offers an innovative framework through which to view response in the perception battlespace. Second, in recognition that coordination is America's current primary liability in counter-influence efforts, this proposal suggests the example of the United States Computer Emergency Readiness Team as a helpful model of public-private partnership from which unified counter-influence efforts can be based.

Alone, this proposal will not bring victory in America's War on Terrorism. In tandem with the right counter-terror policy, however, it is hoped that these ideas will add to the security of the next generation of Americans.

## INTRODUCTION

The most effective path to victory in warfare, as defined in American military doctrine, lies in the neutralization of an adversary's centers of gravity. Such centers of gravity–sources of "moral or physical strength, power, and resistance"–are the heart of the enemy's capability and, resultantly, implicitly become a significant vulnerability (*Joint Publication 3-0: Joint Operations,* 2006, p. IV-10). Historically, centers of gravity have been defined as concentric rings stretching from fielded military forces, to infrastructure, to leadership (Warden, 1995, p. 40-56). The arrival of a new era of conflict in which many of a struggle's most consequential actors interact only outside of the battlefield, however, urgently demands a revision of this guiding premise.

Within the innermost center of gravity in America's global war against terrorist networks stands the will of its population and those of its coalition partners to wage such struggle.[1] How, then, can the United States respond to adversarial influence attacks against this willpower-based foundation of defense perpetrated by transnational Islamist terrorist networks? The following analysis endeavors to explore this fundamental question through understanding of successful influence and counter-influence operations, sufficient historical contextualization, attention to existing military doctrine applicable to the influence challenge, and insight on opportunities to reshape existing institutions and capabilities to better respond to this threat.

[1] Support for this assertion is drawn from the recent writing of cultural critic Michael Novak. Novak concludes, "Today, the purpose of war is sharply political, not military; psychological, not physical. The main purpose of war is to dominate the way the enemy imagines and thinks about the war… The primary battlefield today lies in the minds of opposing publics." See Michael Novak. "What the Islamists Have Learned." *Weekly Standard*, November 22, 2006. Retrieved November 28, 2006, from <http://www.weeklystandard.com/Content/Public/Articles/000/000/012/991gvxyi.asp>

In the five years since America's declaration of a War on Terror, meaningful analysis has been devoted to the role of influence and perception in this conflict. Much of this thinking, however, captures only half of the influence equation: though the United States must certainly work to improve its image through cohesive and credible public diplomacy focused on populations sympathetic to Islamist terrorism, it must also aggressively respond to influence attacks against its own citizens. Beyond strategic framing of freedom, democracy, and globalization, tactical response is necessary to confront images of beheadings, Osama bin Laden videotapes, and media fabrications intended to deceive the American public.

The groundbreaking nature of such tactical counter-influence responses is reflected in the evolving language used to describe this field. Careful observers will note the overlapping domain of ideas identified by terms including information warfare, psychological operations, strategic communications, counterpropaganda operations, perception management, and influence operations. Influence Operations, the broadest umbrella of these ideas, refers to efforts "focused on affecting the perceptions and behaviors of leaders, groups, or entire populations."[2] Reflecting a determination articulated by RAND Corporation researchers Kim Cragin and Scott Gerwher, a reliance on this term stimulates discourse beyond the "means and methods" of an event.[3]

[2] Influence Operations definition taken from *Air Force Doctrine Document 2-5: Information Operations.* (Maxwell, AL: Air Force Doctrine Center, January 2005), 5. Retrieved November 24, 2006, from <http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_5.pdf> Subsets of this idea (as defined in Joint Publication 3-13, *Information Operations)* include Psychological Operations (notably reserved for foreign targets: "The purpose of PSYOP is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives.") and Strategic Communication (most often associated with long-term persuasion efforts coordinated across the government: advancing US interests "through the use of coordinated programs, plans, themes, messages, and products synchronized with the actions of all elements of national power.")

[3] Further discussion on this terminology available in K. Cragin and S. Gerwher, *Dissuading*

Subsequently, in hopes of achieving a framework flexible enough to accommodate innovative terrorist tactics and the broad spectrum of US Government response options, this analysis identifies the defensive and offensive hallmark of perception battlespace as influence operations.

## LITERATURE REVIEW

Canadian journalist and commentator Mark Steyn rightly identifies the nature of the threat posed by Islamist terrorist networks that have exploited the proliferation of Western technology. "The dragons are no longer on the edge of the map: That's the lesson of 9/11," Steyn contends, "When you look at it that way, the biggest globalization success story of recent years is not McDonald's or Microsoft but Islamism… And now, instead of the quaintly parochial terrorist movements of yore, we have the first globalized insurgency (Steyn, 2006)." This understanding of the true nature and scope of the terrorist threat was recently connected to influence manipulation by former Secretary of Defense Donald Rumsfeld:

> There are no armies, no navies, no air forces for our military to go out and soundly defeat in pitched battles on land, sea or air, only rather shadowy networks of vicious extremists who kill other Muslims -- for the most part -- kill innocent men, women and children -- who attack elected governments in an attempt to reestablish a caliphate [sic], and who are increasingly successful at systematically manipulating the world media -- with the goal, the hope, the expectation, and periodically the success, of weakening public will of free people.[4]

*Terror: Strategic Influence and the Struggle Against Terrorism* (Santa Monica, CA: RAND Corporation, 2005), 13-14. Notably, Cragin and Gerwher offer a helpful definition, "An influence campaign uses planned operations—covert and/or overt—to convey selected information and indicators to foreign audiences. Such campaigns attempt to influence the perceptions, cognitions, and behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign behavior favorable to the originator's overall political and strategic objectives."

[4] "Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld at the American Spectator Annual Dinner." *Defense Link News*, November 16, 2006. Retrieved November 24, 2006, from <http://www.defenselink.mil/Transcripts/Transcript.aspx?TranscriptID=3802>

The acknowledgement of the importance of perception in this conflict rests not only in the words of American officials, but also in the public statements of terrorist leaders. As documented by Arizona State University's Consortium for Strategic Communication, Osama bin Laden has concluded, "It is obvious that the media war in this century is one of the strongest methods; in fact, its ratio may reach 90% of the total preparation for the battles (Corman & Schiefelbein, 2006, p. 3)." The recognition by both sides of this conflict of the centrality of influence operations animates the central thrust of this inquiry: how can American defensive strategies, technologies, and institutions better adapt to counter this threat?

Scholarly literature concerning responses to Islamist terrorist influence operations focuses on four key themes. First and most prevalent are accounts of influence operations successfully perpetrated by these terrorist networks. A second field of research characterizes recent counter-influence operations originated or supported by American capabilities. A third perspective presents historical context on the recurring American challenge of coordinating influence response in wartime. A final approach debates policy prescriptions for improved response to these influence events.

### *Conflict in Iraq*

Videotaped beheadings of members of Coalition forces and contractors by Iraqi insurgents stand out as the foremost example of compelling Islamist influence operations projected towards the American population. Sajjan Gohel of the Asia-Pacific Foundation think tank asserts that a key feature of these operations is conduciveness to rapid dissemination and ability to focus attention on one dimension of an event. In a recent

CNN interview concerning this phenomenon, Gohel concluded, “The problems are that the terrorists are very much in power of the media and the propaganda. And that serves their purpose very well, because images are translated to millions around the world (“Your World Today,” 2005).”

Researchers at the U.S. Army War College have identified the logistical mechanisms through which such beheadings become influence operations used to impact targeted populations. In one such circumstance the writers conclude, “The kidnapping of the Turkish workers and posting of the videotape were strategically timed to influence political events and weaken the resolve of NATO.” Based on a timeline assembled by the Army War College writers, this operation intricately unfolded over a 72-hour timespan: “The videotape was aired by *al-Jazeera* on 26 June 2004; an article with a photo was published 27 June and the next day, 28 June, President Bush visited Turkey for the opening of a NATO summit seeking the alliance’s help in stabilizing Iraq (Jones, 2005, p. 8).”

Furthermore, the importance of the perception battlespace is emphasized in consideration of self-inflicted influence harm triggered by American actions in Iraq. The April 2004 emergence of Abu Ghraib detainee abuse photos is a primary instance of this self-defeating phenomenon. Writing in *The Atlantic Monthly*, journalist Mark Bowden concludes, “The photos from Abu Ghraib prison portray Americans as exactly the sexually obsessed, crude, arrogant, godless occupiers that our enemies say we are (Bowden, 2004, p. 37-39).” These images have been exploited in Islamist propaganda materials and stand as a primary instance of the realization that influence does not substitute for policy.

The renaissance of American counter-insurgency doctrine currently unfolding in Iraq provides an excellent case study from which to examine the opportunity of counter-influence operations to shift the course of battle. Existing American military doctrine is based on a cycle of observation, orientation, decision, and action (known as the OODA Loop). Success in executing this determination cycle “faster and more effectively” than an adversary yields the goal of “decision superiority” (*Air Force Doctrine Document 2-5: Information Operations,* 2005, p. 1). As illustrated in the following diagram from the U.S. Army Command and General Staff College, decision superiority in counter-insurgency would allow American counter-influence efforts to intervene in an insurgent’s decision process and potentially alter the outcome of this decision:

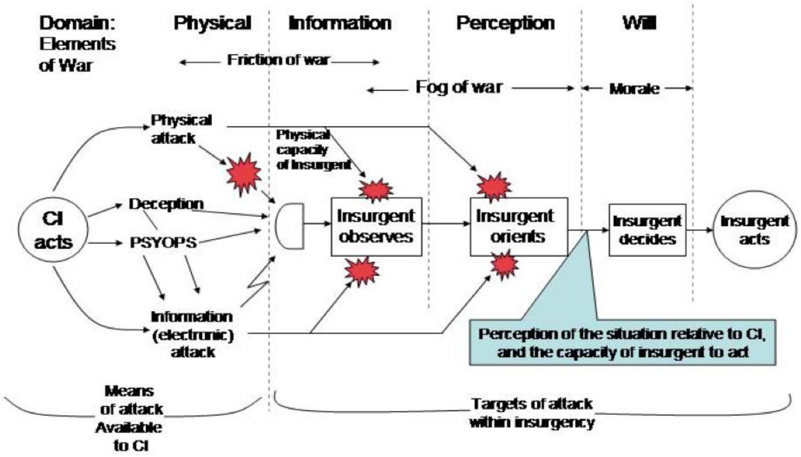
Domain: Elements of War
Physical
Information
Perception
Will
Friction of war
Fog of war
Morale
Physical attack
Physical capacity of insurgent
CI acts
Deception
PSYOPS
Information (electronic) attack
Insurgent observes
Insurgent orients
Insurgent decides
Insurgent acts
Perception of the situation relative to CI, and the capacity of insurgent to act
Means of attack Available to CI
Targets of attack within insurgency

**Figure 1: Modification of Waltz Basic Information Processes Model in a Counterinsurgency**[5]

Assessment of operations in Iraq offers a valuable microcosm illustrative of the importance of a global counter-influence response mechanism.

[5] Robert Molinari, *Winning the Minds in “Hearts and Minds”: A Systems Approach to Information Operations as part of Counterinsurgency Warfare* (Fort Leavenworth, KS: U.S. Army Command and General Staff College), 28. Retrieved November 24, 2006, from <http://stinet.dtic.mil/dticrev/PDFs/ADA436114.pdf>

### *July-August 2006 Israel-Lebanon War*

An additional vivid instance of successful Islamist influence operations occurred in the July-August 2006 Israel-Lebanon conflict. Though the United States was not directly involved in this incident, this instructive example offers insight into both the ease of fabrication of such manipulations and the power of such unchecked propagation. The worldwide headlines resulting from this incident suggested that Israeli missiles had struck two clearly marked Lebanese Red Cross ambulances transporting victims on the evening of July 23, 2006 (Cambanis, 2006). Public reaction to this seemingly flagrant violation of the rules of war dealt an indelible blow to Israel’s justification for the use of force in the conflict. Through the platform of a basic website that was later highlighted on cable news networks, however, an ordinary California-based media consumer convincingly argued that media photos of the ambulance aftermath were not consistent with the story of a missile strike, suggesting a Hezbollah fabrication used to discredit Israel (“Fox Special Report With Brit Hume: Pat Buchanan Releases Immigration Book,” 2006).

Even analysts who accept this instance as an example of the media manipulation and exploitation potential held by decentralized, ideologically motivated groups fail to grasp the gravity of this significance. Beyond the possibility of bias in media reporting and the faults of the 24-hour news stream, this is a case study of a successfully executed influence operation. Accountability in this matter is not the simple responsibility of those that reported and promulgated this deception, but those that created it. What can be done to dilute the effectiveness of such tactics?

### *Nascent Counter-Influence Responses*

Particularly in the case of Iraq, recent experience suggests that some progress is being made in the development of counter-influence tools. RAND Corporation researchers document the emergence of *Iraqi Terrorism in the Grip of Justice,* a nightly Mosul-based television program showcasing captured terrorists and *Al-Hur Al-Ayn*, a television soap opera with effective anti-terrorism themes. While not "silver bullet" solutions, these developments reflect hopeful progress in the perception battlespace.

Furthermore, the American military's discovery and release of a humiliating "blooper" video starring terrorist leader Abu Musab al-Zarqawi suggests a similar experimental tactic seeking to discredit the terrorist. Scenes showing al-Zarqawi's difficulty operating an automatic weapon and training uniform featuring Western sneakers seek to deflate the terror leader's superhero status. Arizona State University researchers explain, however, that the sourcing of this content limited its effectiveness: "While this particular release apparently did not get much traction in the Arab world because it was closely associated with a Western source, it is a good example of what could be done to undermine a terrorist's competence and trustworthiness (Corman, Hess & Justus, 2006, 12)."

In print medium, the exploitation of an intercepted letter between Al Qaeda leader Ayman al-Zawahiri and Iraq-based Abu Musab al-Zarqawi that exposed disagreement over al-Zarqawi's brutal tactics in Iraq is one example of American efforts to factionalize terrorist networks. While the authenticity of the original letter has been legitimately questioned (further emphasizing its role in influence operations), the intent of its exposure appears successful in concerning Americans with the possibility of plans for expanded global jihad, as illustrated in a Pentagon press release highlighting the letter:

> This media battle is why Zawahiri wants Zarqawi to stop attacks on Shiia in Iraq and slaughtering the hostages - they look bad on television… Once the Islamic government is established in Iraq, Zawahiri calls for it to expand into neighboring countries… But the step toward the al Qaeda's version of a perfect world starts with expelling the Americans from Iraq (Garamone, 2006).

Further use of such methods could prove highly effective in creating confusion and dissension in terrorist ranks. Helpfully, such methods also tilt the advantage of surprise in favor of American efforts. A more complete understanding of tactics such as these is reached in the explanation of historical American counter-influence precedent.

### *Historical Precedent of Coordination*

In a paper coalescing his observations as the senior military advisor to the Under Secretary of State for Public Diplomacy and Public Affairs, Army Colonel Brad Ward distinctively captures the historical context of American efforts to create a unified response to adversarial influence operations. “Between World War I and 1986,” writes Colonel Ward, “there were, at least six instances where the US Government created national level Information or Influence type committees (Ward, 2003, p. 12).” These efforts–ranging from World War I’s Creel Committee, to World War II’s Office of Coordinator of Information (COI), to the Korean War-era Operations Coordinating Board, to the last NSC-level coordinating Psychological Operations Committee in 1986–frame a strong American precedent in the influence battlespace. A reach back to the first half of the twentieth century, however, is necessary to locate a definitively responsive American counter-influence coordination attempt, contrasted against broad and ongoing efforts to craft a unified US Government front in public diplomacy.

The September 2002 creation of the Strategic Communication Policy Coordinating Committee represents a powerful step in inter-agency influence and information coordination (Ward, 2006, 15). This group's under-publicized responsibility for "coordinating interagency support for international broadcasting, foreign information programs, and public diplomacy; and promoting the development of strategic communications capabilities throughout government" suggests awareness among senior leadership of the need for an influence strategy. Again, however, even this development lacks the capability of a tactical organization charged with joint response to Islamist terrorist influence attacks.

### *Proposals for Response*

Existing policy proposals to enhance America's influence capabilities largely focus on strategic, long-term efforts focused on reducing general sentiments of anti-Americanism. Often absent from this policy discussion is a consideration of tactical possibilities that could be used to deflect individual influence manipulations perpetrated by terrorist networks. Researchers at Arizona State University's Consortium for Strategic Communication offer one of the few proposals for a tactical response:

> We envision creation of a permanent "geek battalion" dedicated to understanding, monitoring, disrupting, and counteracting jihadi Internet activities. This unit would include to as great an extent as possible young people recruited for their knowledge of Internet culture and technology. (Corman & Schiefelbein, 2006, p. 21)

Columbia University Professor and member of the National Commission on Terrorism Richard Betts buttresses these arguments with an abstract framework calling for American response to these tactics should be predicated on an understanding of the intersection of "the imbalance of power between terrorist groups and counterterrorist governments; the reasons that groups choose terror tactics; and the operational advantage of attack over defense in the interactions of terrorists and their opponents (Betts, 2002, p.

19-36).”  Such a consideration of the dynamic between terrorist groups and counterterrorist governments helpfully frames the doctrinal and institutional recommendations of this analysis.

**MODEL & HYPOTHESIS**

Influence events are subordinate to the backdrop of policy that creates them. Influence response methods rarely overshadow this foundation of policy, a reality seen in the proliferation of unintended negative effects from the April 2004 Abu Ghraib abuse scandal or the self-evident positive outcomes of American aid response to the December 2004 Southeast Asian Tsunami.  Influence response should not be seen as a veneer able to camouflage the true character of American public or foreign policy.  Complete understanding of the influence terrain, however, demands acknowledgement of an active Islamist policy in which influence manipulations play a central role.

The breadth of events and actors within the perception battlespace is overwhelming.  The challenge of simply conceptualizing this non-physical warfare terrain, let alone the possibility of introducing stimulus to affect system-wide change, may seem intractable.  This analysis seeks to focus discussion of response options to a limited type of events within this continuum.  Major applications of the counter-influence posture discussed here include correcting disinformation, limiting the value of kidnappings and hostages, and exposing fabrications.  Admittedly, these strategies are less useful in countering messages directed at the Arab world, silencing general anti-American themes, or fully removing the media spotlight from terrorist action and leaders.

This analysis asserts that the Find-Fix-Track-Target-Engage-Assess (F2T2EA) precision engagement doctrine (*Joint Vision 2010*, n.d., 21) currently employed in

America's battlefield operations can be reinterpreted as a suitable framework to guide a unified US Government response to influence events perpetrated by Islamist terrorist networks. In conventional implementation, the time requirement goal to apply this engagement sequence has been reduced to 10 minutes (Hebert, 2003, p. 50-54). Relying on such precedent, and as visually understood through the diagram below, the time-sensitive nature of this doctrine enhances its applicability to the perception battlespace:

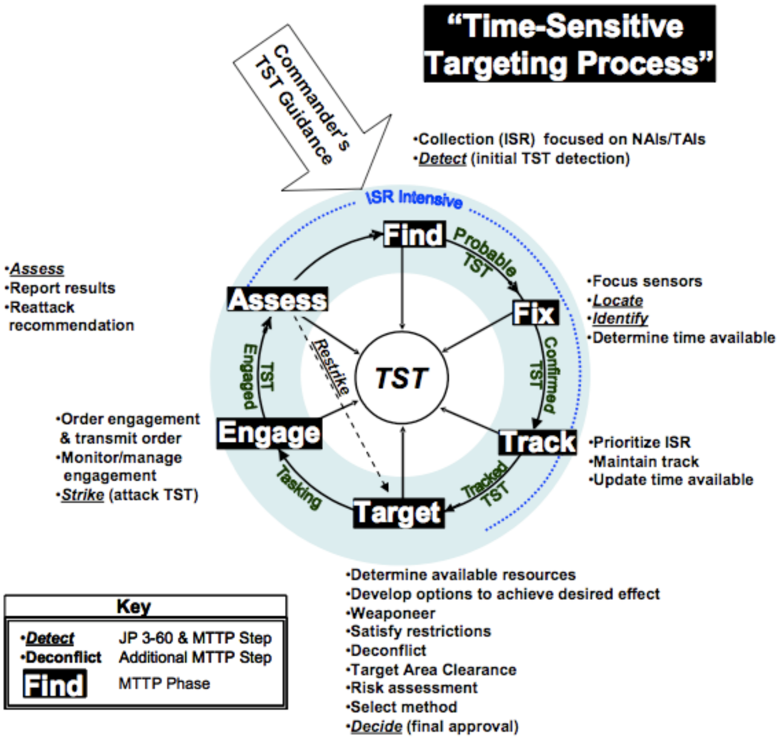

**Figure 2: Time Sensitive Targeting Phases**[6]

Furthermore, this study holds that major requirements of this response framework can be met through reshaping of existing US Government capabilities. Finally, this space will

[6] *Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets*. (Langley, VA: Air Land Sea Application Center, April 2004), I-4. Retrieved October 22, 2006, from <http://www.fas.org/irp/doddir/army/fm2-22-401.pdf>

be used to identify new US Government capabilities that should be developed to address this challenge.

## RESEARCH DESIGN

The application of the F2T2EA model to the challenge of adversarial Islamist influence operations is predicated on a key premise of coordination.  As already emphasized in military doctrine on this subject, "Information operations conducted at the operational and tactical levels may be capable of creating effects at the strategic level and may require coordination with other national agencies (*Air Force Doctrine Document 2-5: Information Operations*, 2005, 1)."  This need for coordination, currently America's biggest liability in counter-influence efforts, begins this new vision.

Unity of command–often cited as the "first among equals" classical principle of war dictates that US Government response to Islamist operations should be coordinated by a central source (Dunlap, 2006, p. 42-48).  A frustrated Army War College student recently identified the current vacuum of such coordination in writing, "Who is in charge of [Information Operations]? Is it the State Department? The DOD? United States Strategic Command (USSTRATCOM)?, United States Special Operations Command (USSOCOM)? Office of Global Communications?, even the Field Artillery Center at Fort Sill, OK has been mentioned as a new major player in IO (Hardy, 2005, p. 7)."

The work of the United States Computer Emergency Readiness Team (US-CERT) provides an instructional example of a public-private partnership established to detect and respond to intrusions.  This agency's charter is responding to cyber attacks—reducing vulnerabilities, disseminating notice of attacks, and coordinating responses–offers a helpful model from which influence operations responses can be based ("United States

Computer Emergency Response Team Announced," 2003). In mirroring the success of this framework, this proposal calls an independently chartered United States Influence Incident Response Integration Center (US-IIRIC) charged with identification, mitigation, and response to influence operations perpetrated by Islamist terrorist networks.[7] A representative example of the sources of expertise available to be drawn on by this organization include:

- Department of Defense "media war" units ("Pentagon Boosts 'Media War' Unit," 2006)
- Joint and Combatant Command units (Such as US Special Operations Command psychological warfare units and the Joint Information Operations Center)
- Service Components (Such as the US Air Force's Operational Cyberspace Command [Bennett & Munoz, 2006])
- Department of State's Bureau of Public Affairs (Including remnants of the US Information Agency absorbed into the Department of State)
- Broadcasting Board of Governors (Responsible for oversight of Voice of America, *al-Hurra*, Radio Free Europe, and other sponsored outlets)
- Intelligence Community (Particularly helpful in contextualizing events, liaison through Office of the Director of National Intelligence)
- Law enforcement and investigative resources (Including the FBI's Cyber Investigations unit)
- Academic expertise (Such as Arizona State University's Consortium for Strategic Communication)
- Military academic expertise (Such as National Defense University's Center for Strategic Communication and service war colleges)
- Contracting services of American political campaign consultants (Moderated through governance of a bipartisan review panel)
- Advisory board of major media organization representatives
- Liaison to pertinent Department of Homeland Security offices

[7] The Defense Science Board Task Force on Strategic Communication has recommended the creation of a similar FFRDC-structured Center for Strategic Communication. This US-IIRIC proposal differs, however, in its mission to respond tactically to discrete influence events. For further information, see *Report on the Defense Science Board Task Force on Strategic Communication.* (Washington, D.C.: Office of the Chairman of the Secretary of Defense, September 2004). Retrieved October 22, 2006, from <http://www.acq.osd.mil/dsb/reports/2004-09-Strategic_Communication.pdf>

While the proposal of a new bureaucratic creation illuminates the impressive array of US Government resources standing ready to meet this challenge, it also exposes the present reality that these tools are uncoordinated, rarely operationalized, and too often under-utilized. Even more important than the organizational structure of this Executive Agent for influence, however, is the doctrine implemented to diffuse Islamist influence operations.

## ANALYSIS & ASSESSMENT

The following assessment seeks to offer practical insight into the implementation of F2T2EA doctrine as a comprehensive framework from which US Government counter-influence actions can be coordinated. Notably, while the necessity for coordination within this effort is self-evident, this position asserts that such doctrine would be best implemented through the proposed US-IIRIC authority but could also be put into practice through existing structures.

Before meaningful response to an Islamist influence operation can be considered, the presence of an unfolding operation must be detected. Criteria should be defined that would separate bona fide Islamist influence operations directed at American or coalition populations from commonplace anti-American "chatter." Consideration of the context of an event (pending democratic elections, military operations, or other policy changes) and the correlation of attack characteristics with known Islamist terrorist methods (symbolism, surprise, power demonstration, and other disproportionate benefits) are examples of dimensions of this determination.

The same persistent Intelligence, Surveillance, and Reconnaissance (ISR) umbrella employed to detect physical terrorist attack offers a comprehensive perspective on nascent influence operations. As such, the existing resources of the Intelligence Community offer the logical starting place from which to mount a lookout for unfolding Islamist influence operations. The proliferation of commercial media analysis products, however, suggests that early open source detection methods may soon offer the capabilities necessary to take the lead in this effort. One such product, CriticalTV, offers technology to automatically flag English and Arabic television whenever certain words are used (Dizard, 2006, p. 1). According to the manufacturer's website, "CriticalTV alerts users about a relevant clip seconds after a broadcast, and allows users to share the clip instantly within a workgroup via secure video-e-mail or a private video gallery. Users can also order a professional transcript or hard copy online (Dizard, 2006, p. 1)." Though not immune from the same potential overload of information that challenges classified collection methods, this technology offers a pragmatic example of the abundance of tools waiting to be utilized in the counter-influence effort.

Once identified as a hostile action, an influence operation must be characterized. Importantly, this level of analysis moves from quantitative observation of an attack's presence to qualitative judgment of appropriate prioritization for response. Unique to the perception battlespace, this characterization requires not only understanding the source of aggression but also discerning the intended target audience and message. Variables of source, motivation, transmission method, and intended audience should be analyzed to gauge the response prioritization level of an event.

Based on this determination of prioritization, an appropriate amount of collection, analysis, and response resources should be tasked with responsibility for the event. An important influence-specific threshold is passed in this tracking process: as many adversarial influence attempts may fail before external interdiction, at what point does the trajectory of this event's success demand response? Given the remarkably dynamic nature of the global perception battlespace, careful attention must be dedicated to monitoring the unfolding nature of this event and the impact of other influence inputs.

After movement through careful periods of identification and observation, response options to reverse, dilute, distract, or otherwise mitigate the effects of an influence operation must be considered. Clausewitz's classic Principles of War offer a starting point from which decisions on method of engagement can be based: objective, offensive, mass, economy of force, maneuver, unity of command, security, surprise, simplicity. Though outside the scope of this analysis, a vital opportunity exists for future scholarship to reinterpret these principles in light of the perception battlespace.

This analysis contends that two tactical response options exist in countering Islamist influence operations. First is a defensive posture that relies upon methods designed to restrict the perpetuation of the original influence operation. Examples of defensive methods include kinetic or electromagnetic attack on broadcast facilities, quarantine of Internet distribution sites, lockdown of funding or logistical support, and containment of radical opinion leaders. Second is an offensive option that seeks to overpower the original influence operation with a counteracting message. Key themes of such remedial messages focus on creating incompatibilities between Islamist action and mainstream Islam, exploiting factional faults between terrorist groups, refuting questionable historical interpretations, and appealing to nationalism or other values.

Influence operations do not occur in a vacuum and can rarely be seen as discrete events. As such, continuing assessment of the effectiveness of countermeasures is essential to mission success. These means and this method of evaluation provides a tenable framework from which the United States can begin to implement an effective counter-influence strategy.

## CONCLUSION

Adversarial influence operations perpetrated by Islamist terrorist networks confront the most foundational of America's national defense capabilities: the will of the American people to fight. While the breadth of this perception battlespace is wide, this analysis has sought to focus attention on a limited scope of influence attacks that can be effectively countered. This assertion is predicated on four key determinations. First, Islamist terrorist networks use influence operations as an integral tool of global jihad. Second, these adversarial influence operations should be perceived as attacks and, subsequently, should demand response. Third, a wide array of US Government tools and institutions currently exists to counter this challenge. Fourth, precision-strike doctrine and cyber-attack response frameworks provide instructional examples of methods to create a coordinated US Government response to such influence attacks.

Examples such as the Hezbollah ambulance incident, beheadings in Iraq, and the exploitation of Abu Ghraib prisoner abuse photos reinforce the reality that influence is a method valued by Islamist terrorist networks. Nascent responses including attempts to discredit terrorist leaders, factionalize terrorist networks, and publicize captured terrorist operatives suggest real progress in American counter-influence efforts. Historical contextualization of these efforts reveals a persistent American challenge of coordinating wartime influence operations, but offers hope in the success of previous generations.

This analysis seeks to bring two new contributions to the counter-influence policy dialogue. First, based on the determination that influence attacks are legitimate matters of national security, this paper recommends response to these events be viewed through the prism of existing military doctrine. Specifically, the same precision-strike doctrine used to neutralize threats with kinetic means offers an innovative framework through which to view response in the perception battlespace. Second, in recognition that coordination is America's current primary liability in counter-influence efforts, this proposal suggests the example of the United States Computer Emergency Readiness Team as a helpful model of public-private partnership from which unified counter-influence efforts can be based.

The possibility of a meaningful counter-influence strategy acknowledges the reality that influence operations reflect but do not replace policy. The methods described in this examination cannot overcome policy failures but can be used to respond to specific instances of aggression towards the American population. The nature of this conflict suggests that only the beginnings of influence manipulations have surfaced as of this writing. A compelling motivation of this proposal, however, is that American policy and institutions must continue to innovate and improve at or beyond the pace of asymmetric threats, such as Islamist influence operations, seeking to harm America. Alone, this proposal will not bring victory in America's War on Terrorism. In tandem with the right counter-terror policy, however, it is hoped that these ideas will add to the security of the next generation of Americans.

## REFERENCES

*Air Force Doctrine Document 2-5: Information Operations*. (2005). Maxwell, AL: Air Force Doctrine Center.

Betts, Richard. (2002) The Soft Underbelly of American Primacy: Tactical Advantages of Terror. *Political Science Quarterly. 117* (1).

Bennett, G. and Munoz, C. (November-2006) "Wynne, Moseley Tap 8th Air Force As First-Ever 'Cyberspace Command'": Inside the Air Force.

Bowden, Mark. (July/August-2004) "Lessons of Abu Ghraib": The Atlantic Monthly.

Cambanis, Thanassis. (July/August-25-2006) Ambulance Drivers Tell Tales of Horror. *Boston Globe.*

Corman, S., Hess, A. & Justus, Z. (2006). *Credibility in the Global War on Terrorism: Strategic Principles and Research Agenda.* Tempe, AZ: Consortium for Strategic Communication, Arizona State University.

Corman, S. and Schiefelbein, J. (2006). *Communication and Media Strategy in the Jihadi War of Ideas.* Tempe, AZ: Consortium for Strategic Communication, Arizona State University.

Cragin, K. and Gerwher, S. (2005). *Dissuading Terror: Strategic Influence and the Struggle Against Terrorism.* Santa Monica, CA: RAND Corporation.

Dizard, Wilson. (November-2006) "FBI Logs On For Monitoring Service For Arabic Networks": Government Computer News.

Dunlap, Charles. (2006) Neo-Strategicon: Modernized Principles of War for the 21st Century. *Military Review. 86* (2).

"Fox Special Report With Brit Hume: Pat Buchanan Releases Immigration Book." (August-14-2006) *Fox News Transcripts.*

Garamone, Jim. (October-17-2005) Al Qaeda Leader's Letter Questions Zarqawi Tactics. *American Forces Press Service.*

Hardy, Charles. (2005). *Information Operations as an Element of National Power: A Practitioner's Perspective on Why the United States Can't Get It Right* . Carlisle, PA: U.S. Army War College.

Hebert, Adam. (2003) Compressing the Kill Chain. *Air Force Magazine. 86* (3).

*Joint Publication 3-0: Joint Operations*. (2006). Suffolk, VA: United States Joint Forces Command.

*Joint Vision 2010*. (n.d.). Washington, D.C.: Office of the Chairman of the Joint Chiefs of Staff.

Jones, Ronald. (2005). *Terrorist Beheadings: Cultural and Strategic Implications.* Carlisle, PA: U.S. Army War College.

*Multi-Service Tactics, Techniques, and Procedures for Targeting Time-Sensitive Targets*. (2004). Langley, VA: Air Land Sea Aplication Center.

Novak, Michael. (2006, November 22) What the Islamists Have Learned. *Weekly Standard.*

"Pentagon Boosts 'Media War' Unit." (October-31-2006). *BBC News.*

"Remarks as Delivered by Secretary of Defense Donald H. Rumsfeld at the American Spectator Annual Dinner." (November-16-2006) *Defense Link News.*

Steyn, Mark. (October-17-2006) A Dark Globalism. *New York Post.*

"United States Computer Emergency Response Team Announced." (September-15-2003) *US-CERT Press Release Archive.*

Ward, Brad. (2003). *Strategic Influence Operations – The Information Connection.* Carlisle, PA: U.S. Army War College.

Warden, John. (1995) The Enemy as a System. *Airpower Journal. 9* (1), 40-56.

"Your World Today." (December-5-2005). *CNN Transcripts.*