The US Army War College Quarterly: Parameters

Volume 39
Number 2 *Parameters Summer 2009*

Article 10

5-1-2009

An Ever-Expanding War: Legal Aspects of Online Strategic Communication

Daniel Silverberg

Joseph Heimann

An Ever-Expanding War: Legal Aspects of Online Strategic Communication

DANIEL SILVERBERG and JOSEPH HEIMANN

Nearly eight years after 9/11, senior US leadership is redefining the "war on terrorism" as a global counterinsurgency effort, one that requires both kinetic force and indirect, "smart power" collaboration by civilian agencies. "The Department of Defense has taken on many of these burdens that might have been assumed by civilian agencies in the past," said Secretary of Defense Robert Gates. "Forced by circumstances, our brave men and women in uniform have stepped up to the task, with field artillerymen and tankers building schools and mentoring city councils—usually in a language they don't speak . . . . But it is no replacement for the real thing, civilian involvement and expertise."[1]

Although the requirement for interagency cooperation is a near-truism of US national security policy today, finding the appropriate role for the Department of Defense (DOD) remains a key challenge. This article examines one aspect of activities that potentially overlap with other government departments, DOD's growing involvement in the "battle of ideas."[2] Much consternation exists in the foreign policy community regarding DOD's expansion into missions traditionally performed by civilian agencies.[3] A small but critical example of this growth involves DOD's efforts to use the Internet to "craft a positive perception" abroad, while attacking the ideological underpinnings of terrorism.[4] In mid-

2007, the Department of Defense issued policies authorizing commanders to engage foreign audiences via online interactive methods, such as texting, blogging, e-mail, and regionally focused Web sites.[5] The guidance was in direct response to long-standing complaints from the ten regional and functional Combatant Commanders that a terrorist could post videos of a beheading or other form of extremist propaganda, unhindered by policy considerations, whereas US commanders had to navigate "legal" hurdles to get psychological operations (PSYOP) videos and themes approved.[6]

A key issue is whether these online activities, while critical to overall American strategic communication efforts, are properly characterized as "military missions," that make use of DOD funding. DOD's communication activities are increasingly separated in time and space from a kinetic mission; are directed at broad, cross-regional audiences; and, on their face, appear more like a public diplomacy campaign than a military program.[7]

It would be unfair to fault DOD for its involvement in such hybrid activities. The Department is arguably filling a need where resource-strapped civilian agencies might be falling short. PSYOP are a key aspect of counter-insurgency efforts. As former participants in and now observers of DOD's expanding communication portfolio, the authors are particularly aware of the argument that the US government needs to respond in real time to extremist propaganda in order to thwart violent extremism and lessen the need for military intervention.

Yet DOD's expansion into the field of interactive communication is troubling on two counts. First, once the Department no longer labels its communication measures as PSYOP, it potentially subverts its own statutory authorities to conduct such programs. The Department has limited authorities to engage foreign audiences, and PSYOP are the principal authorized mechanism to do so. In legal terms, in order to justify the use of appropriated funds, DOD activities are required to support a DOD-specific mission and not conflict with the responsibility of another agency.[8] Once DOD stops calling interactive communication activities PSYOP and undertakes functions similar to those of another department, the "military mission" becomes less defined.

Daniel Silverberg is counsel to the House Committee on Foreign Affairs. He served as an Associate Deputy General Counsel in the Department of Defense Office of General Counsel from 2005 to 2007.

Colonel Joseph Heimann, USAF, is the Senior Appellate Judge on the Air Force Court of Criminal Appeals. He previously was Deputy Legal Counsel to the Chairman of the Joint Chiefs of Staff.

Second, DOD may be encroaching upon the Department of State's mission to engage foreign audiences. The two departments' missions, while overlapping, are distinct. DOD's mission is one of influence; the State Department's mission is one of relationship-building and dialogue. The amalgamation of these tasks potentially undermines the State Department's efforts. At a minimum, it forces one to ask exactly where does DOD's mission end.

The concept of a "war" on terrorism has been extensively analyzed in the context of detainee affairs. Numerous US Supreme Court cases and academic treatises have evaluated the Bush Administration's premise that the United States is engaged in an international armed conflict against terrorist organizations and that detainees are enemy combatants subject to the law of armed conflict.[9] But labeling the ongoing effort a "global war" or even a "worldwide irregular campaign" greatly expands the range of activities that can be justified as a "military mission."[10] Using such terminology might be interpreted as grounds for giving DOD a significant role in areas where the efforts of civilian agencies may be more appropriate.

This article outlines the legal authority for the Department of Defense to conduct communication-related functions; examines how the policy for interactive Internet activities creates a potentially problematic hybrid activity; and assesses whether the policy for the Trans-Regional Web Initiative—an effort to establish a network of regional Web sites—constitutes a tenable DOD mission. The authors conclude that (1) although the authorized activities have potential to be a useful tool in the fight against terrorism, the Department of Defense may need to seek new legal authorities to undertake Internet-based communication; and (2) a conversation needs to take place regarding the degree to which the current configuration should be reworked to protect the missions of both DOD and the State Department and to maximize the efficacy of all US government communication efforts.

Authorized Strategic Communication

The confusion regarding the role and scope of DOD psychological operations in a worldwide irregular campaign stems from a long tradition of ambiguity regarding the relationship between PSYOP, public affairs, and public diplomacy. As a group, these three disciplines are often referred to as "strategic communication."[11]

The State Department's authorities to communicate with foreign audiences are unambiguous and detailed. Among other purposes, including those of the now-defunct US Information Agency, the Secretary of State is statutorily directed to use appropriate media to accomplish the following:

> [P]roperly explain the foreign policy of the United States to the governments and populations of such countries . . . counter misinformation and propaganda concerning the United States . . . [and] continue to articulate the importance of freedom, democracy, and human rights as fundamental principles underlying United States foreign policy goals.[12]

In contrast, there is minimal legislative guidance regarding DOD's authority to conduct information campaigns.[13] Numerous statutes and directives permit the military departments to conduct public affairs, but there are no DOD-focused statutes that define such programs.[14] Similarly, Title 10 of the United States Code, section 167 authorizes the Department of Defense to conduct psychological operations as part of special operations campaigns.[15] But Title 10 does not explain what PSYOP are, nor does it spell out DOD's authority to engage in PSYOP versus public diplomacy.[16]

The primary regulation governing PSYOP is a 1984 DOD directive, "Overt Psychological Operations Conducted by the Military Services in Peacetime," but this document provides minimal guidance.[17] The definition of PSYOP in the directive is sufficiently vague to support numerous activities:

> Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.

As noted by Carnes Lord in his 2006 study, this definition easily could describe a majority of the public diplomacy practices conducted by civilian agencies of the US government, although public diplomacy and public affairs programs never use the term "influence" to characterize their activities.[18]

Among the legislative and regulatory specifications regarding the scope of DOD's PSYOP authority is the legal requirement that a federal department perform only those missions for which it is authorized and funded.[19] This is based on the fiscal law principle that an agency may not expend dollars unless it has authority to do so.[20] The President, as commander-in-chief, may direct the military to act, but the action must fall within an authorized and funded activity. For example, DOD may conduct humanitarian relief operations,[21] even though such assistance clearly overlaps the mandate of the US Agency for International Development, because DOD is authorized to do so within the auspices of Title 10.[22]

DOD's strategic communication efforts also are limited by a "publicity or propaganda rider" inserted annually in the defense appropriation act that prohibits use of funds for publicity or propaganda purposes that are not authorized by Congress.[23] In the absence of statutory defini-

Much consternation exists in the foreign policy community regarding DOD's expansion into missions usually performed by civilian agencies.

tions for PSYOP and public diplomacy, the rider ostensibly limits DOD to conducting publicity or propaganda activities which Congress generally has approved—namely traditional PSYOP or other efforts in support of a military mission.

To the extent a commander uses PSYOP to "shape a battlefield" in direct support of a tactical military mission, such a role would likely be unassailable from a legal vantage point. In fact, commanders who fail to use all available means to influence a battle, including preliminary actions to deter enemy forces or prevent civilian support for the enemy, might be considered derelict. But what happens when the use of PSYOP is not tied to a specific mission? Has Congress authorized the use of DOD funds for generalized, theater-level communication efforts? Is it sufficient to conduct PSYOP under the banner that they support a broad campaign, such as a regional counterterrorism effort, or that they "shape the security environment"? When one eliminates the need for a nexus between communication activities and a specific military mission, such as PSYOP that support troop movement or complement force protection, then PSYOP theoretically can be conducted anywhere, for the broadest of purposes. And that is where DOD is now.

Online Guidance

Confronted by commanders eager to use new media tools to influence foreign populations and a legal landscape marked by an outdated PSYOP directive, then-Deputy Secretary of Defense Gordon England signed two policy memoranda in 2007. The stated purpose of the memoranda is to "provide authority and guidance" for conducting communication through the Internet. The first of these documents, "Policy for Department of Defense (DOD) Interactive Internet Activities,"[24] was signed on 8 June 2007, and the second, "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," on 3 August 2007.[25] The latter policy guidance was promulgated subsequent to a Joint Staff message that had been issued on 5 April 2007.[26]

The memoranda are intended to complement each other.[27] The June policy covers interactive Internet activities (IIA), defined as "the use of a system accessible via the Internet which allows for two-way communications, e.g., e-mail, blogs, chat rooms, and Internet bulletin boards."[28] In other words, the IIA guidance authorizes methods that enable DOD personnel to personally engage with foreign audiences and respond directly to Internet postings, e-mail, and online statements. In contrast, the August policy applies only to "non-interactive content on Combatant Command regionally oriented Web sites tailored to foreign audiences." For example, DOD sponsors Web sites such as maghrebia.com, a news-like Web site focused on the Maghreb that does not allow for interaction between individuals.

So what is the "authority and guidance" for DOD's online activities? To the extent possible, where has the Defense Department drawn the line in cyberspace among PSYOP, public affairs, and support for public diplomacy, and is this line legally defensible?

The Interactive Internet Activities Policy

The 8 June IIA guidance might be viewed as fusing PSYOP and public affairs into a generic communication effort "to provide information to the public, shape the security environment, and support military operations."[29] Interestingly, the policy provides no definitions for these terms, nor does it refer explicitly to PSYOP. Instead, the memo asserts at the outset that IIA are an "essential part" of the listed responsibilities, without distinguishing among them.[30]

The thrust of the IIA policy rests in a delegation of authority from the Deputy Secretary of Defense to the Geographic Combatant Commanders (and Commander, US Special Operations Command [USSOCOM] when designated as the supported commander)[31] to approve IIA "in support of their operations and public affairs activities."[32] The significance of this delegation cannot be overstated. Contrary to two decades of practice, the delegation empowers commanders to conduct information operations at their discretion. Previously they had to seek senior-level Department approval. In essence, this means that a Combatant Commander who wishes to blog on an Arab Web site or exchange e-mails with a Muslim commentator may do so without additional approval.[33]

Scope of Activities

In addition to the delegation of authority, the memorandum spells out two categories of activities to which the policy applies: Public affairs activities and "programs, products, and actions that shape

emotions, motives, reasoning, and behaviors of selected foreign entities." As described in the IIA's statement of purpose, public affairs (PA) involves, in part, "provid[ing] information to the public."[34] The guidance includes a key limitation: Only PA personnel may engage in Internet-based exchanges with journalists. The policy specifically requires:

> Combatant Commanders and [the Assistant Secretary of Defense for Public Affairs] will ensure that only public affairs personnel engage in interactive Internet activities with journalists employed by media organizations including news Web sites, online bulletin boards, and blog sites affiliated with news organizations.[35]

The policy defines media broadly to include "journalists employed by media organizations including Web sites, online bulletin boards, and blog sites affiliated with news organizations" and those individuals and Web sites that have achieved a status equivalent to an established news organization.[36]

Theoretically, there should be little controversy regarding the provision of information to the public or media. Although no specific definition for DOD public affairs exists in statute, Congress has not interfered with DOD's authority to inform the public, foreign and domestic, regarding its activities. From a policy perspective, one would hope that DOD would communicate with foreign media, particularly those in the ever-expanding online arena, to articulate its perspective on events.[37]

Yet the guidance potentially recasts PSYOP-like initiatives as a public affairs activity by authorizing only public affairs personnel to use interactive Internet tools to engage journalists employed by a media organization. The policy restricts who may interact with foreign journalists, but it does not restrict the type of activities in which public affairs personnel may engage. One may presume that public affairs personnel would exclusively employ "public affairs" tools, but the guidance is ambiguous. Thus, the policy could be interpreted as permitting public affairs personnel to engage in "shaping emotions, motives, reasoning, and behaviors of selected foreign entities"—the specified purview of PSYOP practitioners.

Under the new authority, a commander may choose to focus on online outlets "that have become news sources for large audiences" to maximize his effort (why pursue communication with a single blogger when a commander can reach a broader audience?). Thus, the policy would permit public affairs personnel to engage in both PA and PSYOP-like affairs.

In addition to public affairs activities, the IIA guidance authorizes "actions that shape emotions, motives, reasoning, and behaviors of selected foreign entities."[38] This phrasing is curious for two reasons.

But labeling the ongoing effort a "global war" or even a "worldwide irregular campaign" greatly expands the range of activities that can be justified as a "military mission."

First, the language is nearly identical to the definition of PSYOP, except for use of the term "shape" instead of "influence." Second, contrary to the limitation of media contact to "public affairs personnel," the policy does not say who may implement communications that shape emotions and behaviors on behalf of the Geographic Combatant Commander (GCC). In fact, the policy is silent regarding those most likely to use IIA methods—PSYOP forces—whose historical mission is to influence foreign audiences via information operations and whose training involves "motivating" behavior and "shaping" emotions. Although the policy would allow PSYOP forces to add IIA to their list of authorized means of disseminating messages to shape a battlespace, it also potentially allows other personnel—public affairs practitioners and others—to engage in activities traditionally performed by PSYOP specialists.

The ambiguity regarding who will conduct these shaping activities is legally significant for the following reason: Once one amalgamates the public affairs mission to "inform" with the PSYOP mission to "influence," the statutory basis to conduct the activity becomes increasingly dubious. A DOD agenda to "shape emotions" may well overlap with the State Department mission to counter propaganda; both programs involve communicating with foreign audiences in order to positively shape their views of the United States. Once DOD separates IIA from psychological operations and removes a requirement that Internet communication be linked to a specific military mission conducted by PSYOP forces, DOD undermines the very authority it has to conduct such activities, Title 10, section 167. Absent the statutory authority of Title 10, the policy itself simply purports to authorize influence operations that are the equivalent of a State Department function.

Prior to the policy change, DOD exclusively relied upon PSYOP forces to conduct "influence" operations. It trained PSYOP practitioners to work within long-standing regulatory directives that limited the scope of their activities and required extensive oversight. If PSYOP forces are no longer required for online strategic communication, then the training, capability, and oversight tied to the underlying authority are lost.

The blurring of the lines of authority becomes even more acute when a GCC chooses to use contractors to provide IIA support. The new policy expressly permits contractor involvement so long as there is "rigorous US government oversight."[39] Notwithstanding the practical difficulties of providing "oversight" to instantaneous interactive communications such as text messaging and blogging, the policy injects a third group into the mix by authorizing nonmilitary, nongovernmental personnel to engage with foreign audiences.

In summary, the IIA policy empowers commanders to engage in cyber activities away from a battlefield, with personnel who might not be trained in "influence" activities. Perhaps this is a positive development, as DOD is primarily seeking to engage civilian audiences using critical, nonkinetic methods of influence. Yet the breadth of authority bestowed on Combatant Commanders to engage in communication activities raises the question of whether a legislative "fix" is necessary to fully define DOD's responsibilities.

Limitations on IIA Policy

The policy contains four primary limitations.[40] First, it requires that all IIA conducted under its authority "will be accurate and true in fact and intent."

Second, the policy provides that a Geographic Combatant Commander will coordinate IIA with the US ambassador, as appropriate. This caveat could be interpreted in a number of ways. The phrase "as appropriate" possibly means that coordination is necessary only when the GCC assesses that it is. It might also mean that a commander has to coordinate with each ambassador who is accredited to a nation impacted by the IIA. If one pursues the latter interpretation, the limitation potentially causes conflict with existing military programs. Legally, a commander assigned a mission from the President or Secretary of Defense to execute a military operation abroad has no obligation to seek the approval of, or even coordinate with, an ambassador. The GCC decides the limits of the mission to "defend the United States" and the times when it is "appropriate" to consult with the ambassador regarding how the commander attempts to fulfill the mission (in fact, coordination does occur as a matter of prudence and good practice). A requirement to coordinate with the US ambassador thus imposes a restriction on commanders that does not exist in traditional military missions.[41]

Third, the policy has an "attribution" provision. Read in conjunction with the statutory provision restricting DOD's conduct of covert operations, this section simply states a preference for US involvement in IIA to be "openly acknowledged."[42] The policy offers commanders two exceptions. First, it permits a commander to attribute his or her IIA activities to a "concurring partner nation" if the partner nation and the US chief of

Contrary to two decades of practice, the delegation empowers commanders to conduct information operations at their discretion.

mission agree. Second, the policy grants permission to disseminate information via IIA without "clear attribution" in support of a named operation in the Global War on Terrorism or when specified in a Secretary of Defense-approved Execute Order when attribution is not possible due to "operational considerations." The policy stipulates that a commander will disclose US attribution "as soon as operationally feasible." Because a named operation may be geographically broad or nonkinetic, this limitation could empower commanders to engage in clandestine IIA across a wide geographic area. This limitation offers no guidance on where the State Department's or even possibly the Central Intelligence Agency's role and authorities intersect with DOD's in conducting influence operations via the Internet.

Finally, the policy expressly provides that commanders may not delegate the authority granted in the policy. This limitation simply affects who may direct the mechanisms used, and it has no bearing on the underlying substance of the activity.

The IIA policy grants broad authority to GCCs to use IIA in support of their missions. By not specifying who may engage in "shaping operations" or limiting the geographic scope of such activities, the policy in essence establishes a hybrid PSYOP-public affairs model. The activity is, at a minimum, one of publicity, and likely one of propaganda. Yet the personnel engaging in operations to "shape" the emotions and motives of foreign audiences might not necessarily be PSYOP specialists, and the underlying mission itself—to "shape a security environment"—has little definition.

The Trans-Regional Web Initiative

As part of a campaign to counter terrorist influence, US European Command initiated two Web sites in 2007. That program led to the establishment of the Trans-Regional Web Initiative (TRWI), a USSOCOM-led plan to synchronize all Combatant Command Web sites that are tailored to foreign audiences.[43] These Web sites provide news on political happenings, good governance, and other matters of concern to Geographic Combatant Commanders, with the intent of countering hostile propaganda and extremist influence. The TRWI program was approved in a 5 April 2007

message from the Chairman of the Joint Chiefs of Staff, which also includes policy guidance for the TRWI.[44]

The TRWI message states that the regional Web sites are critical to "shaping [a Combatant Command's] security environment" by enabling commanders to reach out to large audiences:

> Web-based operations are an inexpensive and potentially effective method of communicating directly to target audiences with messages shaping the security environment in a Combatant Command's area of responsibility by supporting US interests, the Geographic Combatant Command (GCC) theater security cooperation strategies, the respective country team objectives, and USSOCOM [Global War on Terrorism] objectives. Web sites tailored to foreign audiences can contribute to overall mission accomplishment by countering extremist and terrorist elements, countering hostile propaganda, promoting stability and security, building support for US counterterrorism and associated activities worldwide, and supporting GCC theater security cooperation efforts.[45]

These objectives deserve analysis, as they hint at the amorphous nature of the initiative. The purposes described could refer to a majority of US government activities abroad; any military effort could be said to be justified if it improves the image of the United States. Moreover, the TRWI's objectives explicitly overlap with the State Department's statutory mandate to "explain the foreign policy of the United States to the governments and populations of such countries . . . [and] counter misinformation and propaganda concerning the United States."[46] These goals are arguably the same as the TRWI mission to support US government counterterrorism and GCC theater security cooperation efforts; both involve reaching out to foreign audiences in an attempt to change perceptions regarding America and to counter extremist propaganda. The overlap would not be troublesome if the TRWI supported a specific military mission. Yet the TRWI is, by definition, regional and nonspecific. Unlike a IIA activity, DOD cannot "target" an enemy force with a Web site. In summary, because the TRWI Web sites are by their very nature not in direct and immediate support of military operations, the military mission underpinning these region-wide interests seems ambiguous.[47]

Who Executes the TRWI?

Similar to the IIA memorandum, the TRWI message also provides minimal guidance regarding who executes or maintains the sites. The message unequivocally declares that the TRWI is not a public affairs activity ("[this guidance] does not apply to public affairs Web sites.").[48] While it is possible to foresee a non-public affairs Web site configured in support

of ongoing military operations in Iraq or Afghanistan, DOD's appropriate role becomes significantly less clear when a TRWI-sponsored Web site emerges elsewhere, where combat is not taking place.

The message is also silent on the role of PSYOP forces. Each Web site is required to contain a disclaimer that "clearly identifies the sponsoring Combatant Commander . . . on the homepage of the Web site."[49] Use of .com, .net, and .gov Internet addresses also is specified, unless the Deputy Secretary of Defense authorizes use of other domains.[50] In likely response to the Lincoln Group incident, if a writer is paid for online work, "the article will fully and clearly disclose such payment."[51] In content and appearance, the Web sites resemble formal news sites or diplomatic publications, not military periodicals. Without an indication of who formulates the content and executes the TRWI on behalf of Combatant Commands, it is difficult to discern the precise nature of the activity.

Finally, the "military" aspect of the TRWI becomes increasingly nebulous once third parties are hired to execute the program.[52] In January 2008, USSOCOM issued a solicitation for contractors to perform the sensitive cultural and political tasks inherent in creating and sustaining the Web sites. The notice included the following requirement:

> The contractor shall: Develop, operate, and maintain a minimum of six Web sites, in the directed languages and conceptual approaches approved by the Government; Develop, operate, and maintain Web sites tailored to influence foreign audiences per Government-approved Concepts of Operations (CONOPs), conceptual approaches, and previously approved prototypes; Provide full-service cultural knowledge, political, editorial, media, and information technology capabilities; Identify, develop, obtain, and maintain a network of native/indigenous content contributors with backgrounds in politics, academics, security, culture, entertainment, and other aspects of the [Global War on Terrorism], which appeal to identified foreign target audiences.[53]

One is left to wonder about the military nature of a Web site that is contracted out to civilian, possibly foreign, personnel. From a policy perspective, DOD's sponsorship of the Web sites is troublesome due to the fact that creating such forums requires comprehension of local political events and circumstances, functions typically the purview of civilian US agencies.

Limitations on TRWI Policy

Similar to the IIA, the TRWI policy contains three primary limitations. First, it expressly declares that the authority may not be delegated. Contrary to the IIA policy, however, the TRWI provides a "geographic" limitation when it specifies that Web sites have to be "regionally oriented."

Theoretically, there should be little controversy regarding provision of information to the public.

While the concept of physical limitation on a Web site is illusory, it provides a specification that helps crystallize the question of DOD's authority.

Second, the policy states that a Geographic Combatant Commander will collaborate, as appropriate, with the Department of State, other US government agencies, and country teams in affected nations to coordinate themes and messages, orient to and emphasize specific issues, and recruit regional contributors and key communicators.[54] The caveat "as appropriate" negates the prospect of this limitation resolving the issue of DOD's authority to conduct strategic communication in the place of other government agencies.

Third, the policy has a "transparency" provision. Contrary to the IIA policy that permits different methods of attribution, the Web site memorandum expressly requires that "[a]ll Web sites within the scope of this policy will display a disclaimer link that clearly identifies the sponsoring Combatant Command on the home page of the Web site . . . ."[55] When this requirement is read in conjunction with the statement that the policy does not apply to public affairs Web sites, one is left to question what exactly is the nature of the activity.

Finally, while not a limitation, the policy states that any exceptions, requests for additional authorities, or recommended changes to the policy will be directed to the Deputy Secretary of Defense and that the "Strategic Communication Integration Group Executive Committee" will support the Deputy Secretary in consideration of any such requests.[56]

In summary, the TRWI policy grants broad authority to GCCs to create and maintain Web sites to "shape the security environment" in their areas of responsibility. While these sites require truthful information and complete transparency, they are expressly forbidden from being public affairs Web sites. That stipulation begs the question, what are they? Are they PSYOP being conducted by trained forces in support of a specific mission, or are they public diplomacy sites recast in military terms?

Conclusion

This article highlights a specific example of DOD's expanding mission in the war against terrorism. Arguably, the end goals for US national security agencies, including the State and Defense departments,

One may presume that public affairs personnel would exclusively employ "public affairs" tools, but the guidance is ambiguous.

are the same: Stop extremist activity, thwart terrorist violence, and advance overall US political and economic interests. For a variety of reasons, DOD has assumed control of many of the tools necessary to turn these goals into reality, including strategic communication. The Defense Department's initial efforts to define the authority, scope, and limits of these influence activities are set out in the 2007 policy memoranda. By issuing these memoranda, DOD has significantly blurred its own long-standing distinctions between public affairs and psychological operations. These distinctions were critical in helping military commanders understand the authority and limits of strategic communication efforts. The decision not to define the latest programs as PSYOP raises significant legal questions regarding the authority for DOD to conduct such activities. When DOD expressly does not label these influence operations as PSYOP, has the Department in effect surrendered the authority it has to conduct such operations?

Ultimately, DOD's participation in the "battle of ideas" raises both policy and fiscal questions. In policy terms, DOD may be conducting programs that rightfully belong to another agency. A typical comment today is that the State Department has all the authorities to conduct public diplomacy, but DOD has all the resources. DOD has responded, in kind, by using military terms to define civilian activities for which the Department of State has purview. If DOD is conducting public diplomacy, it should come out and say so. That way Congress knows how appropriated funds are being used, and whether funds are applied for the right purposes, in the most impactful manner.

In dollar terms, DOD's expansion into online strategic communication has potential to further undermine the capacity of civilian agencies, a situation which gave rise to the need for DOD to engage in these activities in the first place. At a certain point, if an agency's mission is viewed as indistinct, that agency's mission becomes a function of the budget process, and the need for funds becomes open-ended.

A new type of PSYOP method may be necessary to fight a "global irregular campaign." It could be a hybrid initiative that draws upon classic forms of military support to public diplomacy and PSYOP.[57] Perhaps existing lines of authority are obsolete and need to be restructured to encompass today's ever-expanding communication methods. Clearly, a structured re-

view needs to take place to determine whether the Department of Defense possesses adequate legal authority to conduct the Internet-based missions necessary in the ongoing fight against terrorism.

NOTES

1. Robert M. Gates, "Landon Lecture" (Manhattan: Kansas State University, 26 November 2007).

2. For a general discussion of DOD's involvement in the war of ideas, see the *National Military Strategic Plan for the War on Terrorism* (Washington: Chairman of the Joint Chiefs of Staff, 2006), http://www.defenselink.mil/qdr/docs/2005-01-25-Strategic-Plan.pdf. See also "Statement of Dr. Michael Doran, Deputy Assistant Secretary of Defense for Support to Public Diplomacy," before the House Armed Services Terrorism, Unconventional Threats, and Capabilities Subcommittee, 15 November 2007. ("The key to the [Countering Ideological Support to Terrorism] mission is influencing a primarily intra-Muslim conversation, with the goal of undermining the intellectual and perceptual underpinnings of terrorism.")

3. For a review of the US military's shift toward nonkinetic missions, see, e.g., Reuben E. Brigety, II, *Humanity as a Weapon of War: Sustainable Security and the Role of the U.S. Military* (Washington: Center for American Progress, 2008), http://www.americanprogress.org/issues/2008/06/pdf/sustainable_security2.pdf.

4. There is much discussion regarding Combatant Commanders playing an active role in the "battle of ideas" between the United States and extremists. See, for example, John M. Myers, "Singular Vision: A Plan to Enable CentCom and State to Work Together," *Armed Forces Journal*, March 2008.

5. See, e.g., "Focus: Moroccan Elections 2007," *Magharebia.com*, http://www.magharebia.com/cocoon/awi/xhtml1/en_GB/special_election2007/awi/special/content/election2007/coverage.

6. For a generic description of the review process, see Chairman of the Joint Chiefs of Staff Instruction 3121.01B, "Standing Rules of Engagement/Standing Rules for the Use of Force for US Forces," 13 June 2005.

7. See Christopher J. Lamb, *Review of Psychological Operations: Lessons Learned from Recent Operational Experience* (Washington: National Defense Univ. Press, 2005), http://www.ndu.edu/inss/Occassional_Papers/Lamb_OP_092005_Psyops.pdf.

8. See *United States v. MacCollom*, 426 U.S. 317 (1976) at 321, in which the Supreme Court reiterated that "the expenditure of public funds is proper only when authorized by Congress, not that public funds may be expended unless prohibited by Congress." See also the Economy Act Agreement for Purchasing Goods or Services, 15 U.S.C. §1535, etc. Pursuant to Federal Acquisition Regulations at 48 CFR 17.502(d), the Economy Act may not be used to make acquisitions that conflict with any other agency's authority or responsibility. See http://www.arnet.gov/far/current/html/Subpart%2017_5.html. See also DOD Financial Management Regulation 7000.14-R, Volume 11A, Chapter 3, *Reimbursable Operations, Policy, and Procedures* (Washington: Under Secretary of Defense [Comptroller]), http://www.defenselink.mil/comptroller/fmr/11a/11a_03.pdf.

9. See, e.g., *Boumediene v. Bush*, 553 U.S. _ (2008); *Hamdan v. Rumsfeld*¸ 548 U.S. 557 (2006); and *Hamdi v. Rumsfeld*, 542 U.S. 507 (2004). For a discussion on the application of the laws of armed conflict, see Benjamin Wittes, *Law and the Long War*: *The Future of Justice in the Age of Terror* (New York: Penguin Press, 2008). The Bush Administration's position regarding the global nature of the conflict may be found in Supreme Court briefings. See, e.g., the US government's brief in *Hamdi v. Rumsfeld*, http://www.usdoj.gov/osg/briefs/2003/3mer/2mer/2003-6996.mer.aa.pdf. ("[T]he military's settled authority to detain captured enemy combatants in wartime applies squarely to the global armed conflict in which the United States is currently engaged, in which—as the September 11 attacks demonstrate—the stakes are no less grave.")

10. The primary focus of the war on terrorism is al Qaeda, which President Bush labeled as a "borderless" terrorist group. See, e.g., George W. Bush, "Remarks on the War on Terror in Tobyhanna, Pennsylvania," 11 November 2005, *Weekly Compilation of Presidential Documents*, 41 (21 November 2005), 1705. ("Many militants are part of a global, borderless terrorist organization like al Qaeda . . . .") Al Qaeda itself characterized its campaign as a global battle. See, e.g., Associated Press, "Al-Zawahri Calls on Muslims to Rise Up in Holy War Against Israel, U.S." *USA Today.com*, 27 July 2006. ("All the world is a battlefield open in front of us.") In turn, numerous commanders and senior Defense Department officials have discussed the war on terrorism as a borderless campaign. For example, see Samantha Quigley, "SOCOM Transforming to Lead Global War on Terrorism," *American Forces Press Service*, 14 March 2006, quoting General Bryan D. Brown, http://www.defenselink.mil/news/newsarticle.aspx?id=15177.

11. See Carnes Lord, *Losing Hearts and Minds? Public Diplomacy and Strategic Influence in the Age of Terror* (Monterey, Calif.: Naval Postgraduate School Press, 2006), 92.

12. 22 U.S.C. §2732. See also the Smith-Mundt Act of 1948 (Pub. L. 80-402, 62 Stat. 6 [1948]) which authorizes the Secretary of State to prepare and disseminate information about the United States through "press,

publications, radio, motion pictures, and other information media." The Department of Defense has no comparable authority or accompanying restrictions.

13. How to differentiate among strategic communication, PSYOP, information operations, and public diplomacy is worthy of a treatise. For the purposes of this article, DOD's online efforts encompass both public affairs and efforts to influence. After all, DOD seeks to influence foreign audiences to not join terrorist groups. PSYOP is thus an appropriate term here. See Lord, 93. Professor Lord points out that the question of whether PSYOP are part of strategic communication is distinct from the issue of distinguishing between public affairs and PSYOP.

14. See, e.g., 10 U.S.C. §3083 (Public Affairs Specialty for the Army). See also DOD Directive 5122.05, "Assistant Secretary of Defense for Public Affairs (ASD(PA))," 5 September 2008.

15. 10 U.S.C §164 also authorizes Combatant Commanders to employ forces, including PSYOP units, in support of their assigned missions.

16. The House of Representatives version of the National Defense Authorization Act for Fiscal Year 2008 (H. R. 1585) inserted the words "information operations" after "psychological operations," perhaps to broaden or clarify DOD's authority, but this revision did not appear in the final enacted text. See the National Defense Authorization Act for Fiscal Year 2008 (Pub. L. 110-181).

17. See DOD Directive S-3321.1, "Overt Psychological Operations Conducted by the Military Services in Peacetime (U)," 26 July 1984. See also DOD Directive 3600.1, "Information Operations," 14 August 2006.

18. See Lord, 94. DOD Directive S-3321.1 also specifies that PSYOP may be used in contingencies short of declared war, defined as "situations determined by [the Under Secretary of Defense for Policy] in which lives of U.S. citizens or property of U.S. Government or U.S. citizens or interests vital to U.S. national security are threatened." This definition could serve as the basis of an antiterrorism-focused PSYOP campaign, but it is also radically broad.

19. See 15 U.S.C. §1535, etc.

20. See *United States v. MacCollom*. See also Timothy Austin Furin, "Legally Funding Military Support to Stability, Security, Transition, and Reconstruction Operations," *Army Lawyer* (October 2008).

21. See 10 U.S.C. §401.

22. See, e.g., 10 U.S.C. §2561.

23. See sec. 8001 of the defense appropriations act for fiscal year 2008 (Pub. Law 110-116; H. R. 3222). ("No part of any appropriation contained in this Act shall be used for publicity or propaganda purposes not authorized by the Congress.")

24. Memorandum from the Deputy Secretary of Defense, "Policy for Department of Defense (DoD) Interactive Internet Activities," 8 June 2007.

25. Memorandum from the Deputy Secretary of Defense, "Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," 3 August 2007.

26. Message from the Chairman of the Joint Chiefs of Staff, "Approval of Trans-Regional Web Initiative (TRWI)," 5 April 2007.

27. The Joint Staff message states that it "applies only to non-interactive content on Combatant Command Web sites tailored to foreign audiences" and that a separate guidance covers "interactive Web-based activities (including but not limited to participation in chat rooms, blogs, and outgoing e-mail)." The message also states that it complements the Trans-Regional PSYOP program, of which the IIA guidance is a key component.

28. "Policy for Department of Defense (DOD) Interactive Internet Activities."

29. Ibid. See "Purpose."

30. Ibid.

31. Based on the Goldwater-Nichols Department of Defense Reorganization Act of 1986 (Pub. L. 99-433), the Department of Defense includes ten Combatant Commands. Four of these commands are "functional" in nature; they have no "Area of Responsibility" and provide special capabilities. The functional Combatant Commands are US Transportation Command, USSOCOM, US Strategic Command, and US Joint Forces Command. The Geographic Combatant Commanders, on the other hand, are responsible for military operations in a specified region of the world.

32. The policy retains for the Assistant Secretary of Defense for Public Affairs the approval authority for all "public affairs" IIA conducted by the Office of the Secretary of Defense and the military departments. For purposes of this article, the authors do not address the use of IIA by either a military department or the Office of the Secretary of Defense. The focus is limited to how a Geographic Combatant Commander may employ IIA in support of his or her mission. It is worth noting, however, that the IIA policy subtly designates the Assistant Secretary of Defense for Public Affairs as the overseer for IIA, a bureaucratic victory for public affairs.

33. The President has assigned the Commander, US Special Forces Command as the lead "for planning, synchronizing, and as directed, executing global operations against terrorist networks in coordination with the other Combatant Commanders." (US Special Operations Command, *USSOCOM Posture Statement 2007* [Tampa, Fla.: US Special Operations Command, 2007], 3.)

34. "Policy for Department of Defense (DoD) Interactive Internet Activities."

35. Ibid., 2.

36. The policy leaves discretion in the hands of a Combatant Commander to determine when the Internet communications of an individual or Web site rises to a level equivalent to a news organization.

37. Congressional investigations, such as the 2006 inquiry into DOD paying foreign journalists to submit "pro-American" stories (the "Lincoln Group" investigation), have centered on the issue of "clandestine" propaganda, not on the issue of DOD's authority to engage with the media.

38. "Policy for Department of Defense (DoD) Interactive Internet Activities," 1.

39. Ibid, 2.

40. The policy also contains an admonishment to comply with all intellectual property laws and a prohibition against conducting commercial activities or endorsement. While important, these caveats are of limited relevance to the question of the scope of DOD's authority in this area.

41. The authors would acknowledge that when it comes to PSYOP activities, the IIA policy only permits a means of dissemination; it is not authority to conduct PSYOP. Unfortunately, the policy does not apply to PSYOP programs only but encompasses a broader scope of activities, for which the IIA policy guidance would provide sufficient authority to execute. The authors are also aware that commanders often coordinate closely and informally with relevant chiefs of mission via the State Department country teams.

42. See sec. 503 of the National Security Act of 1947 (50 U.S.C. §413b). See also "Joint Explanatory Statement of the Committee of Conference," *Congressional Record*, 25 July 1991, H5903-07.

43. In contrast to the IIA guidance, the TRWI guidance applies exclusively to the Combatant Commanders. It grants no authority to the Secretaries of the military departments. ("Approval of Trans-Regional Web Initiative.")

44. Ibid.

45. Ibid., paragraphs 2 and 2.(A).

46. 22 U.S.C.§2732 (c).

47. Moreover, to the extent the mission includes "countering hostile propaganda" and "promoting stability," one should bear in mind that such efforts would be directed broadly at civilian audiences. In fact, al Maghrebia appears as a news site, with sports and political sections. There is no direct targeting of "enemy" or "hostile" forces.

48. "Approval of Trans-Regional Web Initiative," paragraph 2.B.

49. Ibid., paragraph 5.B.(2).

50. Ibid., paragraph 5.B.(3).

51. Ibid., paragraph 5.B.(5).

52. The IIA language requiring "rigorous U.S. Government oversight" is not contained in the August TRWI memorandum. Instead, the memorandum directs that any contract "will fully detail the scope of the work, will not include other communication functions or activities within that contract or task order, and will be fully releasable to the public." ("Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences," 2.)

53. "D—USSOCOM Trans Regional Web Initiative," *FedBizOpps.gov*, 17 January 2008, http://www.fbo.gov/spg/ODA/USSOCOM/SOAL-KB/Reference-Number-SSN01172008/SynopsisR.html.

54. Similar to the requirement to synchronize interactive Internet activities with the commander of USSOCOM, the TRWI memorandum directs Combatant Commanders to "synchronize all Web site material designed to support Global War on Terrorism (GWOT) objectives or to counter ideological support for terrorism with the U.S. Special Operations Command." ("Policy for Combatant Command (COCOM) Regional Websites Tailored to Foreign Audiences.")

55. Ibid, 1.

56. It is the authors' understanding that the Strategic Communication Integration Group was disbanded as of 15 April 2008. The authors are not aware of how the oversight function for TRWI is currently organized.

57. See Lord regarding the revival of a discipline at the Pentagon focused on military support to public diplomacy.