International Journal of Intelligence and CounterIntelligence
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/ujic20

The DNI's Open Source Center: An Organizational Communication Perspective

Hamilton Bean

Available online: 13 Feb 2007

To cite this article: Hamilton Bean (2007): The DNI's Open Source Center: An Organizational Communication Perspective, International Journal of Intelligence and CounterIntelligence, 20:2, 240-257

To link to this article: http://dx.doi.org/10.1080/08850600600889100

International Journal of Intelligence and CounterIntelligence, 20: 240–257, 2007

ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850600600889100

Routledge
Taylor & Francis Group

HAMILTON BEAN

The DNI's Open Source Center: An Organizational Communication Perspective

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD Commission) ceased operations on 27 May 2005, yet its influence reverberates throughout the U.S. Intelligence Community. One of the WMD Commission's high-profile recommendations was to establish an Open Source Center (OSC) within the Central Intelligence Agency (CIA) to ensure that the Intelligence Community maximizes the use of publicly available, foreign print, radio, television, and Internet news and information. Acting on the WMD Commission's recommendation, the Director of National Intelligence (DNI) established the OSC within the CIA on 8 November 2005. Establishment of the OSC indicates that intelligence agencies have struggled to manage public, i.e., "open source," information available to support their missions due to worldwide increases in media content and diffusion of communication technologies. Authorizing legislation for 2006 for the Intelligence Community, the Department of Defense (DoD), and the Department of Homeland Security (DHS) contained explicit references to the problems of managing open source information. The accompanying

Hamilton Bean is a doctoral candidate in the Department of Communication at the University of Colorado at Boulder. His research focuses on organizational communication and national security issues. From 2001 to 2005 he served in management and business development positions for a Washington, D.C.-based OSINT contractor supporting clients within the Intelligence Community. *An earlier draft of this article was presented at the annual meeting of the International Studies Association, San Diego, CA, 22–25 March 2006.*

report to the DHS legislation stated: ''DHS has no comprehensive open source intelligence strategy, despite broad agreement in the intelligence community that better open source intelligence will improve prevention capabilities. The Act establishes a 'one stop shop' within DHS for reliable, comprehensive, and accessible open source information and analysis.''[1]

Similar passages within legislation pertaining to the Intelligence Community and the DoD suggest that the ubiquity of information wrought by technology has led to reconceptions of intelligence work and new debates. The problem of how to manage and demarcate open source intelligence (OSINT) from other types of intelligence and information has sparked disputes within Congress, inside intelligence agencies, and between intelligence agencies and private sector contractors. Witnessing these debates firsthand while serving in management and business development positions for an OSINT contractor that supported the Intelligence Community from 2001 to 2005, I observed the striking disconnect between the discourse surrounding OSINT and its actual production, uses, and effects. Examining OSINT discourse is timely given the WMD Commission's statement that ''many open source materials may provide the critical and perhaps only window into activities that threaten the United States.''[2]

The professional literature typically points to the benefits and limitations of OSINT in meeting intelligence requirements, but larger investigations of how the concept of OSINT functions as an organizational symbol and site of contestation in the intelligence reform debate are absent. Stakeholders, including government officials, policymakers, and contractors should be able to use certain strategies to construct and negotiate the concept of OSINT to meet particular goals and objectives. Yet, this approach still leaves OSINT policies, procedures, products, and services under-discussed, and some may conclude that the concept of OSINT will inevitably be self-defining. As one insider put it, ''Open source will be what the DNI makes it.''[3] But an organizational communication perspective emphasizes the contestation, resistance, and indeterminacy surrounding the creation of meaning, and those forces are active in the case of OSINT.[4]

A BRIEF OVERVIEW OF OSINT

Kimberly Saunders has traced the first modern, institutional effort to manage open source information to World War II and the establishment of the Office of Strategic Services (OSS).[5] She catalogued numerous terms used to characterize OSINT since World War II including: non-secret information; open information; overt information; overt intelligence; public information; unclassified information; and white intelligence.[6] The post-9/11 era has

witnessed a consolidation of this terminology, and now "open source" is the preferred synonym and OSINT the preferred acronym circulating within the government and private sector. Intelligence agencies either perform OSINT activities "in-house" or outsource through contracting. A sample of six publicly available OSINT solicitations included the following focal points:[7]

1. Islamic movements in Indonesia
2. Foreign intelligence services
3. Domestic and international criminal and terrorist organizations
4. Geopolitical, military, scientific, technological, and economic events and developments
5. Perception of U.S. actions and communication, and potential opportunities and vulnerabilities associated with foreign perceptions
6. Specific hard-target adversaries as named by the government

The literature concerning OSINT is limited and much of it tends to promote the field,[8] though some commentators and scholars have offered a critical assessment. Arthur S. Hulnick states that OSINT is the "bread and butter" of analysis, but he also cites contingencies, including information glut, unreliability, misinformation and disinformation, translation requirements, and the availability of the information to adversaries that limit the utility of OSINT.[9] Similarly, Robert Pringle states that OSINT represents a double-edged sword for the government analyst; its inherent ambiguity diminishes its usefulness.[10] Mark Lowenthal highlights how early Intelligence Community attempts to promote the increased use of OSINT failed due to analysts' preferences for classified sources.[11] Stephen Mercado, recognizing that challenge, offers proposals for how to better integrate OSINT into the Intelligence Community.[12] Scholars have examined OSINT in the context of federal policy initiatives, including national competitiveness and the War on Drugs.[13] Others have approached OSINT as a knowledge management or data–mining problem, and investigated the capability of new technologies to make sense of large data sets.[14] Amy Sands states that the Intelligence Community must recognize that it competes with nongovernmental sources for policymakers' attention in the OSINT arena.[15] Like many other commentators, Sands argues that, in order to take advantage of OSINT, the Intelligence Community must devote more human and technical resources to its exploitation.

Amy B. Zegart, Luis Garicano, and Richard A. Posner provide particularly useful concepts drawn from political science and organizational economics to sensitize scholars to the context surrounding the current intelligence reform debate.[16] Zegart provides a theoretical model of intelligence agency adaptation failure. She cites the nature of organizations, the rational self-interest of political officials, and the

fragmented structure of the U.S. federal government as posing serious obstacles to intelligence agency adaptation to a post–Cold War world. Garicano and Posner find that secrecy and centralization contribute to a ''herding problem,'' i.e., intelligence analysts tend to focus on the same limited information when drawing conclusions. The herding problem gets ''locked in'' because the large investments made in intelligence systems prevent information outside that system from entering the analytical process. While intelligence reform can be seen as responding to some of the dilemmas raised by Zegart, Garicano, and Posner, the authors' theoretical models lack explanation of the discursive dimensions that support and sustain their claims. Here is where an organizational communication perspective informs and contributes to theory. Explaining the role of communication improves organizational models in the national security and foreign policy arena. Zegart admits that models drawn from political science and organizational studies leave under-examined the ''routines and cultures'' within government bureaucracies that promote or impede change. Communication scholarship is well-positioned to examine routines and cultures, given the commitment of researchers to focus on the contextualized production and reception of meaning.[17]

With this context in mind, the literature surrounding OSINT can be seen in a new light. Returning to Kimberly Saunders, she stated that her purpose was to present ''what open source information really is,'' and to ''dispel the myths and half-truths that currently exist in the literature....''[18] The focus here differs from Saunders's work and previous studies of OSINT in that stakeholders' attempts to demarcate what OSINT ''really is'' are themselves the subject of inquiry. I argue instead that the ''myths and half-truths'' of the OSINT debate constitute the ''reality'' of OSINT as much as any purported ''objective'' definition.

AN ORGANIZATIONAL COMMUNICATION PERSPECTIVE

Organizational communication is a field of inquiry that examines organizations differently than do managerial, sociological, or economic approaches.[19] Conventional approaches to the study of organizations tend to emphasize efficiency and effectiveness. Organizational communication tends to focus on collective action, agency, messages, symbols, and discourse. Interpersonal relations, communication skills and strategies, organizational culture and symbolism, information flow and channels, and power and influence rank as the most frequently cited topics in the organizational communication literature.[20] Whereas scholars in other fields might see communicating, organizing, and knowing as derivative of more fundamental cognitive or political processes, organizational communication scholars tend to concentrate attention on the former.

In stepping back from a conventional analysis of the organizational contexts of intelligence production, the focus is instead on the organizational discourse shaping the concept of OSINT. In communicating about OSINT, stakeholders are also engaged in reproducing their beliefs about OSINT as a particular category of intelligence. Particularly useful are official statements and congressional testimony recently given before the House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. On 21 June 2005 the Subcommittee held a hearing on *Using Open-Source Information Effectively*.[21] Representative Rob Simmons (R., Conn.), a retired Military Intelligence Officer and longtime advocate for the increased use of OSINT, chaired the hearing. Called to testify were John Gannon[22] of BAE Systems, a former Staff Director for the House Homeland Security Committee before which he was appearing. Gannon is also a former Chairman of the National Intelligence Council and a former Assistant Director of Central Intelligence for Analysis and Production. Eliot Jardines of Open Source Publishing, Inc.[23] and Joe Onek, a senior policy analyst from the Open Society Institute, also testified before the Subcommittee. Nearly six months after the hearing, on 7 December 2005, Jardines was named to the new position of Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS). The hearing transcript is critical to the discussion of OSINT; it is one of the few public records of an actual exchange between OSINT stakeholders in the government and industry.

WHO DEFINES OSINT?

The discourse surrounding OSINT enables stakeholders to agree that government management of OSINT is a critical problem that must be addressed. The discourse also allows multiple goals and objectives to coexist without qualification and prioritization due to the ''strategic ambiguity'' of stakeholders' statements,[24] and it functions to demarcate OSINT from other types of intelligence and information. Analysis of this discourse suggests that key stakeholders are trying to reposition the concept of OSINT in a way that legitimates new institutions, leadership, and funding. Competing definitions of OSINT and claims about its status as a special type of knowledge are being contested among stakeholders trying to demarcate OSINT in specific ways to meet their own goals and objectives.

In terms of competing definitions, Congress supplied a working definition of OSINT in the 2006 Defense Authorization Act:

> (1) Open-source intelligence (OSINT) is intelligence that is produced from publicly available information collected, exploited, and

> disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement. (2) With the Information Revolution, the amount, significance, and accessibility of open-source information has exploded, but the Intelligence Community has not expanded its exploitation efforts and systems to produce open-source intelligence. (3) The production of open-source intelligence is a valuable intelligence discipline that must be integrated in the intelligence cycle to ensure that United States policymakers are fully and completely informed. (4) The dissemination and use of validated open-source intelligence inherently enables information sharing as it is produced without the use of sensitive sources and methods. Open-source intelligence products can be shared with the American public and foreign allies because of its unclassified nature.[25]

A different sense of OSINT is apparent in NATO's definition:

> Open Source Intelligence, or OSINT, is unclassified information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience in order to a address a specific question. It provides a very robust foundation for other intelligence disciplines. When applied in a systematic fashion, OSINT products can reduce the demands on classified intelligence collection resources by limiting requests for information only to those questions that cannot be answered by open sources.[26]

OSINT: An Intelligence Discipline?

These two definitions and the cited congressional testimony indicate a range of interpretations of what constitutes OSINT. Thus, NATO defines OSINT, not an intelligence discipline in its own right, but as a "foundation" for other disciplines. In Congress's definition, OSINT achieves the status of an intelligence discipline, albeit undifferentiated from the others. During the House hearing, Gannon testified that, "Whether [one is] a signals intelligence analyst, or a human intelligence analyst, they all need open source, so you cannot separate it out as a separate discipline, in my judgment."[27] But, Jardines stated, "Over the past 14 years, my career as an open source intelligence practitioner has provided me with an opportunity to understand the significant contributions which the open-source intelligence *discipline* [emphasis added], or OSINT, can bring to the Department of Homeland Security."[28] Longtime OSINT proponent Robert David Steele argues both cases, stating that OSINT "is both a supporting discipline, and an all-source discipline."[29]

Discrepancies about OSINT's status as an intelligence discipline signify differences among stakeholders that lead to problems for OSINT's status as a special type of knowledge. Legitimate intelligence disciplines are given the imprimatur of the Intelligence Community and thus worthy of special

attention and funding. If OSINT is, in former Congressman Simmons's view, "publicly available information that any member of the public can lawfully obtain,"[30] why should it deserve special status as a discipline? The answer is that OSINT is publicly available information and a discipline, as well as myriad other things. OSINT is an object, i.e., the raw data of intelligence, as well as the process of converting that data into useful knowledge for decisionmakers. More importantly, OSINT is also a symbol whose meaning and uses are negotiated by government officials, policymakers, and business leaders to support their respective agendas.[31]

Collecting, Acquiring, or Obtaining OSINT

How OSINT is used as a symbol by different stakeholders is illustrated in an exchange between Eliot Jardines and Rep. Zoe Lofgren (D., Calif.) during the House hearing:

> *Rep. Lofgren*: I think, clearly, we are already making use of open source information, but as I was listening to the testimony I was recalling the debate about thirty years ago about what should be collected by the government and what shouldn't be, and there was a discussion at that time about whether police departments should be allowed to keep files that basically consisted of newspaper clippings. And I thought at the time, well, if it's in the newspaper, anybody can read it, what's the problem with that? And that was, I thought, a sound view. But as technology has moved forward, the ability to compile and amass and integrate information has changed the whole dynamic of what can be found out about people.... So I think we need to think through how this open source dilemma or opportunity meshes with that.[32]

Later, Jardines responded:

> *Jardines*: If I could just add a couple comments here. I'd like to clarify what we're talking about. Open source intelligence is defined as publicly available information. I keep hearing collection from my colleague. Open sources are not collected, they are acquired, which means someone else collects the information, edits the information, and disseminates. The Intelligence Community is merely a secondhand user of that information. So when the congresswoman was mentioning traffic cameras and those kinds of things, all of those fall outside the scope of open source intelligence.[33]

In making a distinction between collection and acquisition, Jardines sought to demarcate OSINT as processed information, rather than raw data.[34] This use of "strategic ambiguity" shielded OSINT from those on the Subcommittee who wanted to use it as a symbol to discuss wider privacy debates.[35] For example, Rep. Lofgren's stated goal was to "protect our nation from terrorism, [and] also protect our citizens from Big

Brother,''[36] but her discussion of privacy issues was precluded. Jardines's distinction between collection and acquisition in the case of OSINT is not universally acknowledged. The WMD Commission Report stated in Chapter 9, ''Regrettably . . . the Intelligence Community does not have an entity that collects (emphasis added), processes, and makes available to analysts the mass of open source information that is available in the world today.'' Representative Simmons offered another verb, stating that OSINT is ''publicly available information that any member of the public can lawfully obtain.''[37] The head of the new OSC, Douglas Naquin, has echoed Simmons: ''Our definition of open source is anything that can be legally obtained.''[38] Semantic distinctions among collecting, acquiring, or obtaining OSINT become critical when stakeholders attempt to demarcate OSINT to protect or promote their agendas.

ASSUMPTIONS ABOUT PUBLIC AND PRIVATE APPROACHES TO OSINT

An important assumption underlying the OSINT debate is that the private sector must play a significant role in OSINT collection, analysis, and dissemination.[39] Dozens of private sector OSINT providers currently support commercial and government clients that have a real financial stake in how OSINT is defined and managed. Depending on how OSINT is defined, the multimillion-dollar industry employs thousands of analysts and marketers worldwide.[40] Then-Representative Christopher Cox (R. Calif.) stated during the hearing, ''It would in fact be a real stretch to suggest that . . . [the] U.S. government could even compete with private sector expertise and outside sources in terms of either quality or currency.''[41] Cox and other stakeholders were able to position their rhetoric in ''culturally sanctioned suspicions'' about government's ability to compete with the private sector.[42] The two witnesses with OSINT experience called to testify were drawn from the private sector. Jardines was a contractor at the time of the hearing, but Gannon had recently served in high-level positions within the government. The Subcommittee did not call a government official with actual responsibility for OSINT to testify; therefore the unstated premise of the hearing was that spurring the ''effective'' use of OSINT within the government is primarily a problem for the private sector to address.

Left under-acknowledged in the OSINT debate was the reality that government and industry ''think'' in two different paradigms. For example, government is interested in centralizing OSINT procurement to reduce costs. ''Pay for it once and only once'' is the maxim heard throughout contracting offices in the Intelligence Community.[43] Yet, private sector OSINT providers benefit from a fragmented market. ''Build it once and sell it many times'' is the mantra of private sector providers; they make

their money at the margins, selling essentially the same service to multiple clients. Private sector providers face the dilemma of trying to achieve economies of scale in a market where each consumer seeks specialized, tailored information. The bottom line is also different for government and commercial clients of private sector OSINT providers. For commercial clients, particularly major international corporations, the value of OSINT is expressed as, ''Did the information make us money or save us money?'' In government, the value of OSINT is expressed: ''Did the information protect national security interests?'' In both cases an assessment of OSINT's value is challenging, but more so in the latter case since the government's bottom line lacks market measures of success.[44]

The fundamental differences between government and the private sector get lost in the discourse about OSINT. For example, Rep. Cox stated, ''Giving the American taxpayer value for money obviously requires using information from open sources whenever possible.''[45] Cox did not distinguish between information collected by government agencies versus contractors. Yet, outsourcing does not guarantee cost savings. Consider Jardines's written testimony: ''It is essential that the all too common 'raping and pillaging' by prime contractors be minimized. The procurement of a $50.00 book should not require a $10.00 pass-through fee and $200.00 in management and administrative charges by the prime.''[46] Practices like these, which contribute to government waste and hurt small businesses like the one Jardines owned at the time of the hearing, prompt him to recommend, ''The final way to integrate OSINT into analytical activities at DHS is to establish a streamlined and specialized contracting process to enable outsourcing of OSINT requirements and commercial content procurement.''[47] In calling for a specialized contracting process for OSINT, Jardines sought to simultaneously demarcate it from other types of information more generally, as well as spur integration between contractors and government agencies. Others questioned how much integration is possible:

> *Rep. Dan Lundgren (R., Calif.)*: Will we run the risk that, when we look to open sourcing, that the Intelligence Community is going to create its own matrix, its own way of getting it, rather than take advantage of those private sector operations that are already out there mining this information? And are these private organizations . . . insufficiently capable of processing that open source information in such a way that it can give that to the Intelligence Community so those analysts can do their work?[48]
>
> *Gannon*: I do think reliance on those organizations is inadequate for the Intelligence Community. I think that the system works best when there is a real partnership, just as you're suggesting, between the analyst dealing with the classified world and then the open source

> world where they tackle a problem together so that they are developing analysis that is continuously integrating the classified with the unclassified.[49]

Gannon's call for a ''real partnership'' and ''continuous integration'' risked minimizing significant problems. Whereas government analysts must hold to a perceived ''intelligence tradecraft,'' private sector analysts are free to expand the boundaries of what constitutes intelligence. For example, in the private sector an analyst may often acceptably make analytical judgments without explicit references to source materials; a commercial client cares primarily whether judgments are accurate. When OSINT contractors offer government clients analytical judgments without explicit references to source materials, considerable tension is often created.[50] This tension is due to the forced tradeoff between ''information quality'' versus ''information efficiency.''[51] When an agency contracts with a private sector OSINT provider, the agency's primary goal is achieving a high level of information quality. Information quality for the government means information and judgments based on the contractor's unique, specialized knowledge and expertise. But quality also means source traceability and accountability because no government official wants to be put in the position of having to back assertions without sources and reasoning. Conversely, private sector OSINT providers are also concerned with information efficiency. The pressure to meet strict deadlines for multiple clients requires that contractors rely on their analysts' professional judgments; source traceability is often of less concern. To cite and organize the source material that influenced an analyst's particular judgment is simply too time-consuming within this project cycle. Private sector OSINT providers are, of course, concerned with information quality, but quality is often oriented to satisfying clients who do not require detailed sourcing. This conceptual dilemma and the economic imperatives separating government and industry make a smooth path to a public–private partnership fraught with difficulty.

COMMUNICATION AND ORGANIZATIONAL STRUCTURE: AN ANALYSIS OF THE OSC

Is the current OSINT debate mere rhetoric? The answer appears to be no. The establishment of the OSC and the ADDNI/OS indicates that major changes are underway. Eliot Jardines has stated, ''The number of open-source items provided in the President's Daily Brief have increased.... I would say we're scoring some wins with our most important customer.''[52] Despite the increased visibility of OSINT, the OSC represents a combination of change and continuity. Specifically, the OSC symbolizes stakeholders' competing positions concerning: 1) the definition of OSINT;

2) the role of the private sector; 3) the continuity of existing structures and processes; and 4) the need for repositioning OSINT as an intelligence resource and organizational symbol. The OSC will collect and study publicly available information from around the world, including media reports, Internet postings and even T-shirts and bumper stickers.[53] OSC material is available to government personnel and contractors through a secure Website. The OSC houses and builds upon the work of the Foreign Broadcast Information Service (FBIS), which was established in 1941 to monitor and translate foreign media. Before its metamorphosis into the OSC, FBIS provided translation, monitoring, and analysis of foreign Internet, print, radio, television, and other sources. Transforming FBIS into the DNI Open Source Center implies a significant change; in order to prevent bureaucratic disruption, however, no consolidation of resources or operational authority under the DNI seems to have occurred.

Jardines's testimony made it clear that the FBIS has historically been underappreciated within parts of the Intelligence Community. He stated: "In part, in the past, with the Community Open-Source Program Office, it wasn't successful primarily because it really wasn't viewed by the rest of the community as a community entity. The leadership and most of the infrastructure was the Foreign Broadcast Information Service, and it simply wasn't accepted as a community-wide effort."[54] Despite this history, General Michael V. Hayden, the then–Deputy Director of National Intelligence, at a July 2005 congressional hearing, stated:

> We do not picture open source being another collection discipline, certainly not in any way beyond what is already being done by FBIS.... So, in essence, the only production line we have is what we have already, which is actually very good. Beyond that, what you get out of the [OSC] is this enabling function that allows the community—frankly, we are not talking about creating anything. We are talking about taking advantage of that which is already out there, if we are only to go out and grab it.[55]

General Hayden, now Director of the Central Intelligence Agency, came down on the side of "non-discipline" for OSINT, thereby maintaining its symbolic status within the Intelligence Community and mitigating the prestige that DNI oversight of OSINT conveys. Will Jardines be able to alter the DNI's position in his role as ADDNI/OS? Is the DNI's immediate attention to OSINT enough to make the OSC a respected part of the Intelligence Community? These are open questions since Jardines acknowledges that FBIS has historically been underappreciated within parts of the Intelligence Community, and the OSC may be interpreted as merely the FBIS with a new name.

In terms of the tension between public and private approaches to OSINT, the OSC paradoxically tilts in the direction of a private sector approach. General Hayden stated: ''I think we picture kind of a SWAT team of experts that can go to a new activity or a new center or a new agency to meet an emerging need to go there and say here is what open source can contribute, let me set up these functions for you, let me advise you along these paths.''[56] Assuming that ''SWAT team'' members are already government personnel, Hayden implied that the OSC is essentially going to mimic the function that private sector OSINT providers have been serving for years, namely, packaging OSINT expertise and capabilities together and selling it as a commodity. The difference is that the OSC appears to be promoting its existing capabilities (i.e., FBIS) rather than building new capabilities since the DNI is ''not talking about creating anything.'' The OSC will focus on services that complement and strengthen component-specific or agency-specific OSINT efforts; it will not serve as a ''one-stop-shop'' for OSINT. This limited role suggests that a major function of the OSC is symbolic since components and agencies will remain free to pursue OSINT support from organizations within or outside the Intelligence Community. Interestingly, Gen. Hayden's rhetoric suggested that it is the government's turn to apply a private sector model in an attempt to solve the problems of OSINT management. Time will tell whether the government's strategy makes OSINT any more useful, integrated, and effective within the Intelligence Community.

Hayden's statement that ''we are not talking about creating anything'' also demonstrated the continuity of processes that existed prior to the hearing and the establishment of the OSC. That should trouble stakeholders who have advocated for more substantive changes within the Intelligence Community. Literature concerning intelligence failure suggests that it is not enough to change organizational structures and expect those changes to impact the work practices and distinctive cultures of intelligence agencies.[57] More than just managing organizational structures, Jardines's mission is to change the culture of the Intelligence Community to value and integrate OSINT. In writing a strategic plan for OSINT, Jardines will have to address not only policies, procedures, products, and services, but also the symbolic ways OSINT circulates within the Intelligence Community. I have indicated where friction points will likely occur.

LINKING ORGANIZATIONAL COMMUNICATION AND INTELLIGENCE STUDIES

Examining the OSC through the lens of organizational communication creates a clearer picture of how OSINT circulates as an intelligence product, process, and organizational symbol shaping and shaped by

underlying organizational structures. The pressure on the DNI to quickly implement WMD Commission recommendations led to creation of the OSC. The organizational structures created to manage OSINT give the appearance of change, yet these structural changes may do little to immediately address more enduring communication issues. As Jennifer B. Sims has noted, even as research validates the importance of decentralized structures and processes in the intelligence arena, bureaucratic reforms stress centralization and new organizational structures.[58] The government seems to have recognized this dilemma in the case of OSINT and has approached change with caution. The OSC leaves distributed approaches to OSINT management intact. Whether that decision is ultimately harmful or beneficial is already the subject of debate.[59]

Some stakeholders argue that, ideally, OSINT obviates much of the need for secret intelligence, while others stress the necessity of collecting and analyzing secret information.[60] According to Michael Scheuer, the former head of the CIA's bin Laden unit, OSINT contains "90% of what you need to know."[61] William Nolte, who recently served on the DNI's staff, puts that figure at 95 percent, as do other commentators.[62] The percentage of useful information available via public sources and the percentage of resources allocated to OSINT exploitation are certainly critical issues. But the OSINT debate turns on a key semantic distinction: does the term "open source intelligence" give intelligence and publicly available information an equivalence that they do not possess? Stephen Mercado recognized this quandary in his essay "Reexamining the Distinction Between Open Information and Secrets."[63] He stated:

> Those who swear that secrets are the only true intelligence, in contrast to mere 'information' found through open means, would do well to consider the indistinct character of the categories of overt and covert in intelligence.... Overt and covert streams of intelligence are by no means completely parallel and distinct; they often mingle and meander over one another's territory.[64]

Despite the blurry distinction, Mercado implied that open information and secrets are not equal. Yet, the fact is that where the demarcation line between "information" and "intelligence" is drawn has much to do with stakeholders' persuasive appeals, and less to do with any intrinsic quality of the information itself. For instance, early last year a senior official on the DNI's staff was overheard to assert that there is no such thing as "open source intelligence"—there is only "information"—and this official did not want to hear the term OSINT used anymore.[65] In the long run, the status and legitimacy of OSINT and other types of intelligence relates to the degree to which members of the Intelligence Community, individually and collectively, believe these terms are equivalent or exceptional.

THE QUESTION REMAINS UNANSWERED

The fields of organizational communication and intelligence studies have been united in an effort to explain herein the discourse about OSINT currently circulating within the government and private sector. A focus on competing definitions and assumptions about OSINT reveals that the OSC, intended to implement the recommendations of the WMD Commission, does little to resolve important underlying issues in the OSINT debate. The OSC represents a negotiation, a first step at translating competing positions into tangible structures and action. According to many policymakers and government officials, United States national security may depend on OSINT. Yet, a fundamental question remains: what constitutes OSINT and how is it distinguished from other types of intelligence and information? In creating a strategic plan for OSINT, Eliot Jardines has had to confront that question, but he alone cannot answer it. Many stakeholders will also try to answer that question, but any answer is likely to be partial, contingent, and based on individual and collective perceptions and objectives.

REFERENCES

[1] United States Congress, House of Representatives, *Department of Homeland Security Authorization Act for Fiscal Year 2006*, 109th Cong., 1st sess., H.R.1817.

[2] Laurence Silberman and Charles Robb, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, March 2005. URL: http://www.wmd.gov/report/

[3] John Gannon, personal communication with author, 10 April 2006.

[4] Dennis K. Mumby and Cynthia Stohl, ''Disciplining Organizational Communication Studies,'' *Management Communication Quarterly*, Vol. 10, No. 1, August 1996, pp. 50–72.

[5] Kimberly A. Saunders, ''Open Source Information: A True Collection Discipline'' (M.A. thesis, Royal Military College of Canada, 2000).

[6] *Ibid.*

[7] Solicitations are available from *Federal Business Opportunities*. URL: http://www.fedbizopps.gov

[8] See Alessandro Politi, ''The Citizen as 'Intelligence Minuteman,'" *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 1, Spring 2003, pp. 34–38; Robert David Steele, *The New Craft of Intelligence: Personal, Public and Political—Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption* (Oakton, VA: OSS International Press, 2002).

[9] Arthur S. Hulnick, ''The Downside of Open Source Intelligence,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 15, No. 4, Winter 2002–2003, p. 565.

[10] Robert W. Pringle, ''The Limits of OSINT: Diagnosing the Soviet Media, 1985–1989,'' *International Journal of Intelligence and CounterIntelligence*, Vol. 16, No. 4, Summer 2003, pp. 280–289.

[11] Mark Lowenthal, ''Open Source Intelligence: New Myths, New Realities,'' *Intelligencer*, Vol. 10, No. 1, February 1999, pp. 7–9.

[12] Stephen C. Mercado, ''A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age,'' *Studies in Intelligence*, Vol. 48, No. 3, 2004, pp. 45–55; Stephen C. Mercado, ''Reexamining the Distinction Between Open Information and Secrets,'' *Studies in Intelligence*, Vol. 49, No. 2, 2005.

[13] Denis A. Clift, ''National Security and National Competitiveness: Open Source Solutions,'' *American Intelligence Journal*, Vol. 14, No. 2 and 3, Spring/Summer 1993, pp. 25–28; J. F. Holden-Rhodes, *Sharing the Secrets: Open Source Intelligence and The War On Drugs* (Westport, CT: Praeger, 1997).

[14] Jami M. Carroll, ''OSINT Analysis Using Adaptive Resonance Theory for Counterterrorism Warnings,'' in *Artificial Intelligence and Applications Conference held in Innsbruck, Austria 14–16 February 2005*, H. M. Hamza, ed. (Calgary: ACTA Press, 2005), pp. 756–760.

[15] Amy Sands, ''Integrating Open Sources into Transnational Threat Assessments,'' in *Transforming U.S. Intelligence*, Jennifer E. Sims and Burton Gerber, eds. (Washington, DC: Georgetown University Press, 2005), pp. 63–78.

[16] Amy B. Zegart, *Flawed by Design: The Evolution of the CIA, JCS, and NSC* (Stanford, CA: Stanford University Press, 1999); Amy B. Zegart, ''September 11 and the Adaptation Failure of U.S. Intelligence Agencies,'' *International Security*, Vol. 29, No. 4, 2005, pp. 78–111; Luis Garicano and Richard A. Posner, ''Intelligence Reform Since 9/11: An Organizational Economics Perspective,'' *Journal of Economic Perspectives*, Vol. 19, No. 4, Fall 2005, pp. 151–170.

[17] Thomas R. Lindlof and Bryan C. Taylor, *Qualitative Research Methods*, 2nd ed. (Thousand Oaks, CA: Sage, 2002).

[18] Kimberly A. Saunders, *Open Source Information*, p. 8.

[19] Dennis K. Mumby and Cynthia Stohl, ''Disciplining Organizational Communication Studies,'' *Management Communication Quarterly*, Vol. 10, No. 1, August 1996, pp. 50–72.

[20] Phillip K. Tompkins and Maryanne Wanca-Thibault, ''Organizational Communication: Prelude and Prospects,'' in *The New Handbook of Organizational Communication: Advances in Theory, Research*, Frederic M. Jablin and Linda L. Putnam, eds. (Thousand Oaks, CA: Sage, 2001), pp. xvii–xxxi.

[21] United States Congress, House of Representatives, Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information Effectively: Hearing before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment*, 109th Cong., 1st sess., 21 June 2005.

[22] I worked for Intellibridge Corporation as a client account manager during Dr. Gannon's tenure with the company in 2001.

[23] Eliot Jardines sold the company prior to his appointment as ADD/OS.

[24] Eric M. Eisenberg, "Ambiguity as Strategy in Organizational Communication," *Communication Monographs*, Vol. 51, September 1984, pp. 227–242.

[25] United States Congress, House of Representatives, *National Defense Authorization Act for Fiscal Year 2006*, 109th Cong., 1st sess., H.R.1815, p. 1.

[26] NATO, *Open Source Intelligence Handbook;* available from http://www.oss.net

[27] United States House of Representatives, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source*.

[28] *Ibid*.

[29] Robert David Steele, *Information Operations: Authors Briefing*, 2005. URL: http://www.oss.net

[30] Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information*.

[31] Susan L. Star and James R. Griesemer, "Institutional Ecology, 'Translations' and Boundary Objects: Amateurs and Professionals in Berkeley's Museum of Vertebrate Zoology, 1907–39," in *The Science Studies Reader*, Mario Biagioli, ed. (New York: Routledge, 1999), pp. 503–524.

[32] United States House of Representatives, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source*.

[33] An Intelligence Community insider remarked to the author that Jardines's distinction is critical since intelligence agencies limit OSINT collection, even on suspected terrorists, to a perceived restriction under Executive Order 12333, particularly if information resides on a server that may be owned by a U.S. citizen or is physically located within the U.S.

[34] Jardines poses an intriguing question, namely, does raw data posted on the Internet become data that has been collected, edited, and disseminated?

[35] See Gordon R. Mitchell, "Another Strategic Deception Initiative," *Bulletin of the Atomic Scientists*, Vol. 53, March/April 1997, pp. 22–23; Gordon R. Mitchell "Whose Shoe Fits Best? Dubious Physics and Power Politics in the TMD Footprint Controversy," *Science, Technology, & Human Values*, Vol. 25, No. 3, Winter 2000, pp. 52–86.

[36] United States House of Representatives Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information*.

[37] *Ibid*.

[38] Susan B. Glasser, "Probing Galaxies of Data for Nuggets," *The Washington Post*, 25 November 2005, p. A35.

[39] Shane Harris, "Intelligence Incorporated," *Government Executive Magazine*, 15 May 2005, pp. 40–47; Shane Harris, "Intelligence Shop," *Government Executive Magazine*, 1 May 2005, URL: http://www.govexec.com/features/0505-01/0505-01na3.htm

[40] Representative companies include, but are not limited to: Open Source Solutions; Open Source Publishing, Inc.; The Economist Intelligence Unit; Jane's Information Group; Eurasia Group; Stratfor; Oxford Analytica; East View Information Services; Booz Allen Hamilton; Kroll Inc.; Pinkerton Consulting; iJET Travel Intelligence, Inc.; Medley Global Advisors; and Toffler Associates Inc; See also *Quarterback Consulting, The Private Intelligence Industry Report* (Cheshire, CT, 2003).

[41] United States House of Representatives, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information*.

[42] Charles Conrad, ''The Illusion of Reform: Corporate Discourse and Agenda Denial in the 2002 'Corporate Meltdown,'' *Rhetoric & Public Affairs*, Vol. 7, No. 3, Fall 2004, pp. 311–338.

[43] My experience working with Intelligence Community officials and contracting officers supports this assertion.

[44] Luis Garicano and Richard A. Posner, ''Intelligence Reform.''

[45] Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information*.

[46] Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information;* written testimony of Eliot A. Jardines.

[47] These practices hurt small businesses by forcing them to either pay significant ''pass-through'' fees to the prime contractor, or pass those fees on to the customer, which may make the price of service prohibitive.

[48] Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information;* written testimony of Eliot A. Jardines.

[49] *Ibid.*

[50] The author witnessed numerous instances where government officials deemed commercial OSINT products unsatisfactory for lacking source material for key assertions. It made no difference that analysts producing the assessments were considered experts in their fields.

[51] William D. DeLone and Ephraim R. McLean, ''The DeLone and McLean Model of Information Systems Success: A Ten-Year Update,'' *Journal of Management Information Systems*, Vol. 19, No. 4, Spring 2003, pp. 9–30; Larry P. English, ''Information Quality: Critical Ingredient for National Security,'' *Journal of Database Management*, Vol. 16, No. 1, March 2005, pp. 18–33.

[52] Patience Wait, ''Intelligence Units Mine the Benefits of Public Sources: Open Source Center Draws, Analyzes Info from a Variety of Public Databases,'' *Government Computer News*, 20 March 2006. URL: http://www.gcn.com/print/25_6/40152-1.html

[53] Susan B. Glasser, ''Probing Galaxies of Data for Nuggets,'' p. A35.

[54] Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, *Using Open-Source Information*.

[55] Congress, House, Permanent Select Committee on Intelligence, Subcommittee on Oversight, *DNI Status: Hearing before the Permanent Select Committee on Intelligence, Subcommittee on Oversight*, 109th Cong., 1st sess., 28 July 2005.

[56] *Ibid.*

[57] Amy B. Zegart, "September 11 and the Adaptation Failure of U.S. Intelligence Agencies."

[58] Jennifer E. Sims, "Transforming U.S. Espionage: A Contrarian's Approach," *Georgetown Journal of International Affairs*, No. 6.1, Winter/Spring 2005, pp. 53–59.

[59] See commentary on OSS.net website.

[60] Some of the materials contained on the OSS.net website could be interpreted as advocating for OSINT as a replacement for traditional intelligence in certain instances.

[61] Susan B. Glasser, "Probing Galaxies of Data for Nuggets," p. A35.

[62] William Nolte, *The Intelligence Community in the DNI Era: A One-year Assessment*, paper presented as part of the panel "Intelligence Community Reform, One Year After" at the annual meeting of the International Studies Association, San Diego, CA, 22–25 March 2006. URL: http://www.isanet.org/sandiego/; also see Stephen C. Mercado, "Reexamining the Distinction Between Open Information and Secrets."

[63] Stephen C. Mercado, "Reexamining the Distinction Between Open Information and Secrets."

[64] *Ibid.*

[65] Intelligence Community insider, personal communication with author, 22 March 2006.