

SUMMER 2007

International Journal of Intelligence and CounterIntelligence, 20: 240-257, 2007  
Copyright © Taylor & Francis Group, LLC  
ISSN: 0885-0607 print/1521-0561 online  
DOI: 10.1080/08850600600889100



Handwritten notes:   
DIA  
EMERSON  
GRAY - USMC  
ASPIN. BROWN  
INT'L  
OPEN SOURCE'S  
97 - SUTTON  
MAY 2007

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.*

WNA  
EIS  
MARC

DNV  
2007

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."<sup>1</sup>

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."<sup>2</sup>

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."<sup>3</sup> 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.<sup>4</sup>

W/INSTR  
EIS  
MAICRS '15

GOOD

### 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).<sup>5</sup> 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.<sup>6</sup> The post-9/11 era has

OSINT  
S/O