Order Code RL34270

CRS Report for Congress

Open Source Intelligence (OSINT): Issues for Congress

December 5, 2007

Richard A. Best, Jr.
Specialist in National Defense
Foreign Affairs, Defense, and Trade Division

Alfred Cumming
Specialist in Intelligence and National Security
Foreign Affairs, Defense, and Trade Division

Congressional Research Service

Prepared for Members and Committees of Congress

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
05 DEC 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Open Source Intelligence (OSINT): Issues for Congress	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service, The Library of Congress,101 Independence Ave SE,Washington,DC,20540-7500**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**27**	

Open Source Intelligence (OSINT): Issues for Congress

Summary

Open source information (OSINT) is derived from newspapers, journals, radio and television, and the Internet. Intelligence analysts have long used such information to supplement classified data, but systematically collecting open source information has not been a priority of the U.S. Intelligence Community (IC). In recent years, given changes in the international environment, there have been calls, from Congress and the 9/11 Commission among others, for a more intense and focused investment in open source collection and analysis. However, some still emphasize that the primary business of intelligence continues to be obtaining and analyzing secrets.

A consensus now exists that OSINT must be systematically collected and should constitute an essential component of analytical products. This has been recognized by various commissions and in statutes. Responding to legislative direction, the Intelligence Community has established the position of Assistant Director of National Intelligence for Open Source and created the National Open Source Center. The goal is to perform specialized OSINT acquisition and analysis functions and create a center of excellence that will support and encourage all intelligence agencies.

The effort has been only underway since late 2005 but the Center is up and running, and providing support, including training, to OSINT professionals throughout the Intelligence Community. Administrative mechanisms are in place to ensure that there is a comprehensive community-wide open source effort. It appears, however, to some observers that not all agencies have as yet made comprehensive commitments to acquiring and using open source information, nor that the ODNI has taken sufficient steps to ensure that open sources are appropriately exploited. Observers suggest that congressional oversight of the OSINT process might provide insight into current progress as well as identify areas that need modification. A particular focus of congressional interest might be potential tradeoffs between classified and open source collection to ensure that needed information is obtained in the best and most cost-effective manner. Proponents maintain that this approach helps to ensure that agents and expensive surveillance systems are focused on obtaining information that is being actively hidden.

The collection and analysis of OSINT information will be ultimately judged by its contribution to the overall intelligence effort. Collecting information from open sources is generally less expensive and less risky than collection from other intelligence sources. The use of OSINT may result not only in monetary savings but also in less risk than utilizing sensitive technical and human sources. OSINT can also provide insights into the types of developments that may not be on the priority list for other systems or may not be susceptible to collection through other intelligence approaches — innovative applications of new technologies, shifts in popular attitudes, emergence of new political and religious movements, growing popular discontent, disillusionment with leadership, etc. Supporters of OSINT maintain that the future contribution of the Intelligence Community will be enhanced by its ability to provide detailed information and incisive analyses of such developments. This report will be updated as new information becomes available.

Contents

Open Source Intelligence (OSINT): Issues for Congress

Introduction

Although the Intelligence Community has received its share of criticism since its formal establishment in 1947, it appears such criticism has intensified since the end of the Cold War as the Community confronted a string of perhaps unprecedented challenges, including those from the dissolution of the former Soviet Union, the 9/11 terrorist attacks, and the 2003 Iraq War and its aftermath. Although each of these events triggered demands for Intelligence Community reform, perhaps no single change in the past quarter of a century can match the enduring, day-to-day challenge posed by the information revolution. Twenty five years after the development of the Internet and the personal computer, the explosive impact of the this technology-driven change continues to ripple through the Intelligence Community.

One result of this revolutionary change has been a newfound willingness on the part of the U.S. Intelligence Community to reexamine the extent to which it relies — or has failed to rely — upon open source information, which some have argued has been relegated to a "second class" status by many intelligence professionals who continue to value secret information above all else. As part of this reexamination, the Intelligence Community appears to be reassessing a number of open source issues, including the relative value of open source information compared to that of secret information; the impact and importance of the growing volumes of information unlocked by easy access to the Internet; the dampening effect that certain Community security practices may have had and may continue to be having on the use of open sources; the state of development of analytic tools necessary to effectively and efficiently collect, sift, analyze, and disseminate a vast volume of publicly available information when analysts are expected to also analyze increasingly large amounts of classified information; and, training issues relating to open source technology and techniques.

If the global information revolution has sparked debate within the Intelligence Community over the value of open source information, the ongoing jihadist terrorist threat has sharpened its focus. In underscoring the strategic and tactical importance of open source information generally, and the role of the Internet specifically, one senior policymaker recently described the Internet as being America's new open source battlefield.[1] Those who share this view tend to argue that the Intelligence Community must improve its strategic understanding of the of the jihadist threat by

---

[1] See comments of Francis Townsend, Assistant to the President for Homeland Security and Counterterrorism, DNI Open Source Conference, July16-17, 2007, Washington, D.C.

more effectively mining the Internet and other open sources for information. Such an effort, it is suggested, also will enable the Community to achieve a better tactical understanding of how jihadists use the Internet's web-television capabilities, chat rooms, and "news" sites, to train forces and raise money. Ultimately, these observers suggest, the United States must develop the capability to understand and influence foreign populations — "not in their council of states but in their villages and slums" — if it is to effectively counter the threat posed by jihadists. In such circumstances, it is argued, the information that should matter most to policymakers can be derived from open sources.[2]

The debate over the relative value of open source information, compared to that of classified data, is occurring at a time when the global information environment is viewed by some as having reached a "post-modern" stage.[3] In such an environment, secret information may be less important than the combination of open source information, information sharing, computer networking, and an ability to sift and analyze a dizzying volume of open source information. Indeed, one former senior intelligence officer suggested that whereas the 20th century was the century of secrets, the 21st century may well prove to be the century of global information. If the Intelligence Community as a whole accepts and understands this change, according to some observers, it may gain an edge in confronting current threats, particularly those posed by terrorism.

Debate Centers on Relative Value Of Open Source

Intelligence professionals generally agree that open source information is useful and that such information should be collected and analyzed, just as is data derived from classified sources. They disagree, however, over its value relative to that of clandestinely-collected secret information, and thus the amount of time, attention, and resources that should be devoted to its collection and analysis remains in dispute. For a brief case study of open source intelligence, see Appendix.

There generally are three different prevailing views regarding the of relative value of open source information. The first holds that policymakers simply derive less value from such information than from clandestinely-collected secrets. While open source information can complement, supplement and provide context for classified data, such information, it is suggested, rarely provides insight into an adversary's plans and intentions. Policymakers tend to view such information as being critically important to policy deliberations, and attach to it the highest value. For that type of insight, it is argued, the Intelligence Community must discover and collect secrets. It therefore is entirely appropriate that the Community target the

---

[2] George Parker, "Knowing the Enemy; A Reporter at Large," *The New Yorker*, December 18, 2006, p. 69.

[3] Stevyn Gibson, "Open Source Intelligence, An Intelligence Lifeline," *RUSI Journal*, February 2004, p. 17.

preponderance of its resources to that end. As the Director of Central Intelligence (DCI) reportedly stated in 2005, "I only have money to pay for secrets."[4]

The second view asserts that open source information should be viewed not only as an important contextual supplement to classified data, but also as a potential source of valuable intelligence, in and of itself. Proponents of this view tend to cite the as-Sahab Institute, al-Qaida's sophisticated Internet-based messaging and propaganda multimedia production facility, as an example of why open source collection and analysis is so important in today's technology-driven and globalized world.[5] Others cite al-Qaida's ability to use virtual space to recruit, proselytize, plot, and plan with impunity.[6] According to one observer, "al-Qaida is right on the cutting edge of the adoption of new technologies. They grab hold of the new stuff as soon as it becomes available and start using it."[7] Another commentator suggested that gaining an understanding of the inner workings of the as-Sahab Institute may provide as an effective way as any "to get close to bin Laden and Zawahiri."[8] According to one former senior intelligence who believes that the Intelligence Community continues to undervalue open source information, "[Open source information] is no longer the icing on the cake, it is the cake itself."[9]

Proponents of the third view adopt a "middle-ground" position, arguing that open source information probably will never provide the "smoking gun" about some issue or threat, but that it can be instrumental in helping analysts to better focus or "drive" clandestine collection activities by first identifying what is truly secret. Open sources therefore should be viewed as an analyst's "source of first resort." Although these adherents tend to champion the relative value of open sources, their supports appears to be measured. While generally believing that the Intelligence Community should devote additional resources to collecting and analyzing open source information, they appear wary of over-selling its value. "We don't have the confidence yet," according to one senior intelligence officer, in explaining such wariness.[10]

---

[4] See Ronald A. Marks, "Spying and the Internet," *The Washington Times*, April 25, 2005, p. A-21.

[5] See Shaun Waterman, "As-Sahab: al Qaida's Video Production Unit," *United Press International*, September 20, 2007.

[6] See Arnaud de Borchgrave, "Networked and Lethal," *The Washington Times*, September 25, 2007, p. 18.

[7] Ibid.

[8] Ibid.

[9] Interview with former senior intelligence official, June 6, 2007.

[10] See comments of Mary Katherine Graham, Deputy Director of National Intelligence/Collection, Director of National Intelligence Open Source Conference, July 16-17, 2007, Washington, D.C.

Historically, Open Source Has Played a Secondary Role

Although the Intelligence Community has long utilized open source information, some suggest that the Community has been slow to recognize its value, for two reasons. First, the Intelligence Community's principal mission is to discover and steal secrets; relying on open sources runs counter to that mission. Second, it is suggested that the Intelligence Community views clandestine-collected information as being more valuable because it is more difficult to collect.[11] As one observer of the Intelligence Community commented, "[Open source] was seen as irrelevant, and [the Intelligence Community] much preferred working with spies and satellites."[12] Because of this bias, the Intelligence Community has been viewed as supporting and investing in collecting and analyzing open sources only on the margins.

Ironically, any failure by the Intelligence Community to more fully appreciate the importance of open source information may have occurred despite some senior intelligence officers acknowledging its value at various times. For example, Sherman Kent, the Intelligence Community's legendary analyst, estimated that in peacetime 80 percent of the information policymakers needed to make decisions was available publicly.[13] Lt. Gen. Samuel V. Wilson, former director of the Defense Intelligence Agency, provided an even higher estimate, asserting, "Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond."[14]

Since the onset of the information revolution, and in the aftermath of the Cold War, the Intelligence Community's reliance on open source information grew as the Internet expanded and the availability of public information increased dramatically. The world also became more open. For example, in the case of Russia, it is estimated that the ratio of unclassified to classified information in the case of Russia has more than reversed from its 20:80 cold war ratio.[15]

---

[11] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), p. 64.

[12] Benjamin Wallace-Wells, "Private Jihad," *The New Yorker*, May 29, 2006, P. 38.

[13] Memorandum Respecting Section 202 (Central Intelligence Agency) of the Bill to Provide for a National Defense Establishment, Submitted by Allen W. Dulles, April 25, 1947, reprinted in U.S. Congress, 80th Congress, 1st session, Senate, Committee on Armed Services, *National Defense Establishment (Unification of the Armed Services)*, Hearings, Part 1, page 525.

[14] Donna O'Harren, "Opportunity Knocking: Open Source Intelligence For the War on Terrorism," Thesis, Naval Postgraduate School, December 2006, p. 9.

[15] See Mark M. Lowenthal, *Intelligence, From Secrets to Policy, Second Edition*, CQ Press (Washington, D.C.), 2003, p. 80. Even at the height of the Cold War, a period of time when the Intelligence Community focused much of its efforts on clandestine collection against the former Soviet Union, American intelligence analysts made time to track the publishing records of Soviet scientists. They highlighted when certain scientists stopped publishing for a period of time, concluding that any such pauses could signify that the Soviets were developing new technologies. Such pauses would trigger new targeting aimed at determining

(continued...)

With the end of the Cold War, the Intelligence Community's reliance on open source information also grew because it turned its attention away from the sophisticated military programs of the Soviet Union and towards the disparate threats posed by emerging post-Cold War threats. Collection strategies shifted from sophisticated surveillance satellites capable of counting tanks and missiles to the gathering of whatever information was available on rogue states and terrorist groups. Much of the information found was actually openly available but not hitherto collected and analyzed. The shift within the intelligence agencies was publicly championed by open source advocates such as Robert Steele of Open Source Solutions, who has conducted annual conferences to bring together open source experts from around the world and written extensively on the topic.[16] In addition, intelligence agencies have come to utilize and rely on electronic databases and search engines which were developed for civilian markets. Some contractors have developed software and other research tools specifically for sale to intelligence agencies.

While acknowledging that the Intelligence Community is relying more on open source information, some observers insist that the Community continues to undervalue such information while focusing most of its attention on collecting secret information. Joseph Nye, a former head of the National Intelligence Council in the 1990s, perhaps best captured the prevailing view of the Intelligence Community when he stated, "Open source intelligence is the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle...open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort."[17]

Some open source proponents view such information as constituting more than just the "the outer pieces of the jigsaw puzzle," but rather every bit as valuable as clandestinely-collected secrets.

Open Source Information Defined

Definitions of "open source information" have varied over time. Most simply, the term refers to information that is unclassified. It also has been defined to signify information that is derived from overt, non-clandestine or non-secret, rather than hidden or covert collection. The Intelligence Community defines open source information as that information that is publicly available material that anyone can

---

[15] (...continued)
if new technology was under development. See Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), pp. 67-68.

[16] See Robert D. Steele, *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, VA: AFCEA, 2000).

[17] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), pp. 67-68. p. 64.

lawfully obtain by request, purchase, or observation.[18] Thus, the acquisition of such information must conform with extant copyright requirements.

Although open source information consists of unclassified material, the Intelligence Community sometimes classifies certain open source information that it collects, including information provided by substantive outside experts, if it determines that the process by which the information is collected could reveal intelligence sources and methods, intelligence requirements for certain collection of intelligence, or certain policy concerns.[19]

Open source information, according to some observers, generally falls into four categories[20]: widely available data and information; targeted commercial data; individual experts; and "gray" literature, which consists of written information produced by the private sector, government, and academe that has limited availability, either because few copies are produced, existence of the material is largely unknown, or access to information is constrained.[21] Within these four categories, open source information can include:

- media such as newspaper, magazines, radio, television, and computer-based information;
- public data such as government reports, and official data such as budgets and demographics, hearings, legislative debates, press conferences, and speeches;
- information derived from professional and academic sources such as conferences, symposia, professional associations, academic papers, dissertations and theses, and experts;[22]
- commercial data such as commercial imagery; and,
- gray literature such as trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, and market surveys.[23]

---

[18] Intelligence Community Directive Number 301 and P.L. 109-163, Sec. 931.

[19] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), p. 65.

[20] Ibid, p. 65.

[21] Ibid, p. 65.

[22] See Mark M. Lowenthal, *Intelligence, From Secrets to Policy, Second Edition*, CQ Press (Washington, D.C.), 2003, p. 79.

[23] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), pp. 64-65.

Open source information also can include information, which although unclassified, could be considered company proprietary, financially sensitive, legally protected, or personally damaging.[24] With increasing frequency, it also includes information derived from Internet blogs. According to Intelligence Community officials, blogs are providing "a lot of rich information that are telling us a lot about social perspective and everything from what the general feeling is[,], to ... people putting information on there that doesn't exist anywhere else."[25]

There continue to be misconceptions about open source information, even, it is suggested, among intelligence officials. One such misconception is that intelligence analysts rely on the Internet for most open source information. In fact, according to a 2003 published estimate, analysts derived only three to five percent of such information from Internet sources.[26] It should be noted that there could be any several reasons for this low estimate, including the lack of open source expertise; ineffective analytic tools; a lack of subject expertise; deadline pressures that prevent more extensive evaluation of Internet sources; the possibility that the Internet may not provide the best sources for certain needed information; or, some combination of these factors.

Another misconception is that open source information is free. Although such information can be collected, certainly at less expense than, for example, than that collected by satellite, the Intelligence Community, like any other consumer of various media, still must pay for access. The Community also must purchase analytic tools that enable analysts to more effectively sift open source information. And the Intelligence Community is increasing its investment in analytic tool development. For example, the Department of Defense recently awarded Johns Hopkins University a $48 million grant to develop technology that is capable of automatically translating and analyzing speech and text in multiple languages. It is generally believed that the Intelligence Community must achieve such a capability if it is to effectively collect and analyze open source information.

When does open source information become "open source intelligence?" According to the statutory definition, such information becomes "intelligence" when it is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement.[27] The definition refers to "collection," even though some open source analysts prefer to use the term "acquired," arguing that analysts generally acquire previously collected and publicly available information second-hand. Most intelligence professionals, however, employ the term "collection."

---

[24] Ibid, p. 65.

[25] See Bill Gertz, "CIA Mines 'Rich' Content From Blogs," *The Washington Times*, April 19, 2006, p. 4.

[26] See Mark M. Lowenthal, I*ntelligence, From Secrets to Policy, Second Edition,* CQ Press (Washington, D.C.), 2003, p. 80.

[27] P.L. 109-163, Sec. 931. Intelligence Community Directive Number 301.

Analysts Face Obstacles in Use of Open Source

Intelligence analysts confront several obstacles in making more effective use of open source information. One such obstacle — perhaps a principal one — is that many analysts lack sufficient subject matter expertise. Indeed, open source proponents assert that open source intelligence is as much about such expertise — foreign language and cultural understanding — as it is about the underlying data itself, and that it would be misleading to assume that the value of such intelligence exists mostly, or solely, in the information itself.

Another such obstacle can be the analyst's own bias against open source information. Some analysts believe that such information generally is not as carefully vetted as clandestinely-collected intelligence and therefore is less creditable, and ultimately provides less value to the policymaker. Thus, driven by deadlines and confronted by large volumes of open source and classified information, analysts often choose to focus their limited time and resources on analyzing clandestine-collected intelligence. Moreover, they often receive further encouragement to do so from managers who establish priorities that favor the analysis of clandestinely-collected secrets.

Other obstacles include:

- Training. Analysts often lack the training necessary to make the most effective use of open sources.

- Internet on the desktop. An unknown number of analysts and collectors still are unable to access the Internet from their desktops. That any analyst or collector lacks Internet access leads some observers to question the Intelligence Community's commitment to more fully developing open source capabilities.

- Volume. In searching open sources, analysts confront an enormous volume of information. Identifying and analyzing information from this data stream can be daunting, and analysts must rely upon their subject matter expertise and an effective set of analytic tools to tackle the task. Volume, however, also can work in an analyst's favor. By being able to check multiple sources, an analyst is better able to assess whether a certain piece of information is deceptive, biased, or in error.

- Tools. The search for more effective analytic tools remains a challenge. Analysts continue to be overwhelmed by text searches that require examination and correlation. In addressing this problem, the Intelligence Community trying to develop visualization tools that will better enable analysts to more effectively extract and manipulate critical information from all available information sources.

- The "echo" effect. Such an effect occurs when more than one media outlet makes available the same news story. The resulting repetition can imbue a particular news item with more credibility and

importance than is warranted. Given the proliferation of news sources, this phenomenon remains a continuing challenge for analysts.

- Security. According to some observers, overly rigid Intelligence Community security practices continue to limit the broader and more effective use of open source information. Certain practices — for example, polygraph requirements and classification reviews of subsequent publications — can discourage outside experts from collaborating with Intelligence Community counterparts. Subsequently classifying information provided by outside collaborators can also undermine cooperation. Such practices have a "dampening effect," according to some critics.[28] Security officials acknowledge as much, but generally argue that security concerns must take precedence.

Intelligence Community Criticized For Not Making Greater Use of Open Source

Over the past decade, two national commissions criticized the Intelligence Community for its failure to promote the use of open source information and a third recommended that an open source center be established that would serve the Community. The commissions also criticized the Community's preferential bias with regard to classified information.

Aspin-Brown Commission

In 1996, the Aspin-Brown Commission criticized the Intelligence Community for failing to make greater use of open source information.[29] The commission, established by Congress to review the Intelligence Community's post-Cold War effectiveness, concluded that the Intelligence Community was moving too slowly to provide analysts access to open source data bases, particularly given the volume of information readily available on the Internet.

While noting that the development of open source data bases was growing, the Commission said that intelligence analysts had only limited access to such data bases. The Commission criticized the Community for an effort that it characterized as "inexplicably slow" and recommended that a computer infrastructure be established that connected intelligence analysts into open source information networks. Although

---

[28] See "Preparing for the 21st Century: An Appraisal of U.S. Intelligence," *Commission the Roles and Capabilities of the United States Intelligence Community*, March 1, 1996, p. 88. The Commission is referred to as the Aspin-Brown Commission, in recognition of the Commission's leaders, former Congressman Les Aspin and former Secretary of Defense Harold Brown.

[29] Ibid, p. 88.

the Commission did not address the issue of funding for open source, it did urge the Intelligence Community to adopt less intrusive security measures.

9/11 Commission

In contrast to the Aspin Brown Commission's more detailed treatment of the open source issue, the 9/11 Commission's final report only briefly mentioned the topic of open source information. Its final report contained a diagram outlining a new Intelligence Community organizational chart that proposed the establishment of an open source center within the Central Intelligence Agency (CIA)[30] but did not further explain the concept. Commissioners reportedly viewed open source information as important but lacked sufficient time to more fully explore the issue.[31]

WMD Commission

The WMD Commission, formally known as The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, concluded in a 2005 report that the Intelligence Community makes too little systematic use of outside experts and open source information.[32] As did its 9/11 Commission counterparts, the WMD commissioners recommended that a open source center be established within CIA.

In making this recommendation, commissioners concluded that:

> Analysts have large quantities of information from a wide variety of sources delivered to their desktops each day. Given the time constraints analysts face, it is understandable that their daily work focuses on using what's readily available — usually classified material. Clandestine sources, however, constitute only a tiny sliver of the information available on many topics of interest to the Intelligence Community. Other sources, such as traditional media, the Internet, and individuals in academia, non-governmental organizations, and business, offer vast intelligence possibilities. Regrettably, all too frequently these "non-secret" sources are undervalued and underused by the Intelligence Community.[33]

Commissioners recommended that analysts broaden their information horizons and encouraged them to expand their use of open source material, outside experts, and new and emerging technologies.

Congress Urges Creation of an Open Source Center

Following the completion of the 9/11 Commission report but in advance of the publication of the WMD Commission's final report, Congress in 2004 approved a

---

[30] The 9/11 Commission Report, 2004.

[31] Interview with 9/11 Commission staff.

[32] The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, March 31, 2005, p. 389.

[33] Ibid, p. 395.

comprehensive intelligence reform bill that included a "Sense of Congress" resolution calling for the establishment of an open source center which would collect, analyze, produce, and disseminate open-source intelligence.[34] The resolution described open source intelligence as a valuable source of such information that must be integrated into the intelligence cycle to ensure that the U.S. policymakers are fully and completely informed.

Intelligence Community's Response: the Open Source Enterprise

Greater emphasis on open source information came in the wake of the Intelligence Reform and Terrorism Protection Act of 2004 (P.L. 108-458) which included the most extensive changes in intelligence organization since 1947. The act stated that open source intelligence is "a valuable source that must be integrated into the intelligence cycle to ensure that United States policymakers are fully and completely informed." It also expressed the sense of Congress that the Director of National Intelligence (DNI) should establish "an intelligence center for the purpose of coordinating the collection, analysis, production, and dissemination of open-source intelligence to elements of the intelligence community." The act asked for a report by June 30, 2005, from the DNI containing his decision on whether an open source center is advisable.

In response to this congressional direction, the Administration opted to establish a National Open Source Enterprise built around several key principles:

- the establishment of the position of Assistant Deputy Director of National Intelligence for Open Source with overall oversight responsibility of the open source effort;
- coordination by the Office of the Director of National Intelligence (ODNI) for open source funding requests in the DNI's budgetary submissions and allocations;
- the creation of a "Guild" of open source experts at an Open Source Center and by ensuring that open source competency becomes an Intelligence Community requirement;
- a single open source requirements management system to balance resources and acquisitions against priorities;
- establishment of a single open source architecture to facilitate access to a wide range of potential consumers at federal, state, local, and tribal levels; and

[34] Section 1052, P.L. 108-458.

- creation of an entity to develop and acquire cutting-edge technologies and processes that advances efforts to acquire and utilize open source information.[35]

General Hayden, then the Deputy DNI, described the new approach to a subcommittee of the House Permanent Select Committee on Intelligence (HPSCI) in July 2005 as setting up an "enabling function" to encourage the effective use of open source information throughout the Intelligence Community. Hayden stated:

> . . . what we're talking about is a center that has the expertise that can advise us in the community on the information technology and the policy changes that will be needed to allow every analyst in the community access to open source information.
>
> . . . we picture a kind of a SWAT team of experts that can go to a new activity or a new center or a new agency, or 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.[36]

National Open Source Center (NOSC)

The unfolding of the Administration's plan to establish a National Open Source Center (NOSC) began on November 1, 2005 when the Center was officially and publicly established by the DNI. Administratively, it was placed under the management of the CIA and its organization incorporated and augmented the Foreign Broadcast Information Service (FBIS) which has provided open source products to the government and outside researchers since February 1941. According to a DNI press release, the Center's functions include "collection, analysis and research, training, and information technology management to facilitate government-wide access and use." Located in suburban Northern Virginia, the NOSC currently has several hundred full-time personnel some of whom are on temporary assignments in other agencies. Although NOSC remains under the administrative control of the CIA, the aim is to provide a center of expertise for the entire government in exploiting open source information. It can be tasked by other agencies for specific research efforts.[37]

NOSC provides translations and transcriptions of media products from around the world. NOSC translations and analytical products are currently available online in a website (*opensource.gov*) that is available to government officials. Many of these

---

[35] See Office of the Director of National Intelligence, Intelligence Community Directive 301, *National Open Source Enterprise*, July 11, 2006.

[36] Testimony of Lt. Gen. Michael Hayden, Deputy Director of National Intelligence, to the Oversight Subcommittee of the House Permanent Select Committee on Intelligence, July 28, 2005, Federal News Service transcript.

[37] See Hamilton Bean, "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence*, Summer 2007; also, Robert K. Ackerman, "Intelligence Center Mines Open Sources," *Signal*, March 2006.

products are also available to the public or to outside experts through the World News Connection, a commercial news service.[38] The NOSC maintains a vast collection of published material in electronic form, including daily downloads of hundreds of newspapers and journals.[39]

The NOSC seeks to establish higher professional standards for open source collection and analysis, to create an open source "guild." Although every analyst knows about some open source materials such as the local newspaper, the rapidly expanding availability of electronic databases and a large variety of search strategies requires extensive training and skills that only IT specialists are likely to acquire in graduate schools. It is widely maintained that training in specific searching skills is cost effective as it reduces time-consuming and unproductive searches.

Use of Open Source in Government Agencies

A fundamental goal is not just to hire more open source practitioners but to alter agency cultures to ensure that use of open source information is a routine and natural component of analytical practice. Changing agency cultures is a formidable task. As one intelligence scholar has noted:

> The culture of the intelligence community tends to devalue the use of open sources except in marginal ways. In part because open sources are by definition available to the public, they remove one of the psychological benefits of being an insider with special information. Relying on classified information immediately limits those with whom an analyst can discuss issues and creates a wall between those with access and those without it. Intelligence analysts must, by law, exclude outsiders without clearance from access to classified information; but in this way they create an exclusive club that inhibits the use of relevant and potentially significant expertise. Also, as noted earlier, many intelligence analysts trust only classified information. They may put excessive confidence in such materials, perhaps in the belief that they have been closely vetted and validated during the collection process. This stamp of approval for classified information, and the bias favoring it over other sources, can cause analysts to be closed off to data emerging from researchers who use open sources.[40]

To some extent, resistance to the use of open source information may be more prevalent among analysts whose careers began during the Cold War when the focus was on secretive nation states with sophisticated military capabilities. Analysts who have entered the workforce in more recent years will have had routine access to open source information in academic environments or in previous professional

---

[38] See [http://wnc.fedworld.gov/description.html].

[39] Much of this information appears in online versions that is removed after a few days; NOSC performs an essential service by archiving key website publications for future reference.

[40] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), p. 72.

assignments.[41] Thus they may be more inclined to continue routine use of open sources in conjunction with classified data.

A major component of the open source initiative has, nevertheless, been an effort to ensure that open source experts are available and utilized in all intelligence agencies and at the same time avoid unnecessary duplicative efforts. This effort has concentrated on enhancing expertise within the NOSC and in offering training for open source experts in other agencies. In many cases, however, the number of persons whose job responsibilities focus on, or include open source information to a significant degree have not been consistently identified.

The ODNI's budgetary authorities may permit decisive support to the open source effort. Dedicated open source positions at appropriate paygrades could do much to ensure the visability of the open source effort. With information expected to be available from individual agencies and reviewed by the ODNI, budgets submitted by the DNI each year could include more detailed information on specific open source analyst positions in each agency. Congress would then have the opportunity to review these efforts through the budget process to ensure adequate, but not redundant, open source capabilities. Some argue that open source billets should be identified not only in national intelligence agencies but also in military intelligence agencies.

Information sharing, based on state-of-the-art information technology, is another important part of the effort. The Open Source Center manages this effort for the entire Intelligence Community as well as homeland defense partners at the state, local, and tribal levels. The goal is to maximize connectivity throughout the Government and to supercede separate agency-based system that have incompatible formats and extensive duplicative materials. Individual agencies may continue to maintain independent open source databases, but the goal is that they are maintained in formats that can be accessed by analysts at other agencies. The WMD Commission noted that "Information technology has made remarkable advances in recent years. The private sector (without the same kinds of security concerns as the Intelligence Community) has led the adoption of technologies that are also critical to intelligence. Two areas show particular promise: first, machine translation of foreign languages; and, second, tools designed to prioritize documents in their native language without the need for translation."[42]

This effort depends heavily on the expertise and initiative of commercial enterprises to develop useful and cost-effective technologies. In 1999 the CIA developed In-Q-Tel to to provide a means for business firms to work with intelligence agencies on comparatively small contracts. The effort has been widely praised but has been largely focused on classified technologies. A similar approach,

---

[41] Clive Thompson, "Open-Source Spying," *New York Times Magazine*, December 3, 2006 describes the frustration felt by some newly-hired analysts coming into intelligence agencies several years ago only to discover that computer access to intelligence literature and the search engines used in intelligence agencies reflected decades-old technologies.

[42] *WMD Commission Report*, p. 396.

but one focused solely on unclassified open source technologies has been proposed for implementation by the ODNI.

One of the most important sources of information from non-governmental sources private sector contributors is commercial imagery that is purchased by the National Geospatial-Intelligence Agency. Commercial satellites provide extensive overhead coverage of targets throughout the world to supplement imagery from government satellites. In some cases it has also meant that overhead imagery of significant quality is available to anyone with access to the Internet. Although the background and extent of this use lies beyond the scope of this Report, the use of commercial imagery has had a major influence on the intelligence community, especially on the procurement and operation of government satellites.[43] Commercial imagery, however, is a special case as the Government is in the many cases the principle customer. For most other open source information, the U.S. Government is only an incidental customer (and in some cases an undesired one).[44]

Department of Defense (DOD)

The Defense Department has long been an important center of open source information. The Asian Studies Detachment (ASD) in Camp Zama, Japan has collected and analyzed open source information on Far Eastern topics since 1947. With the services of U.S. military personnel and Japanese civilians, the ASD translates and analyses information for military commands in the region and makes its products available to the Intelligence Community.[45] Other military commands, some not technically part of the Intelligence Community, also undertake open source collection and analysis. Although the introduction of web-based information sharing systems makes it possible to share such information with other DOD and IC users, incentives to share information have not always been present.

In the wake of the 9/11 Commission Report and during consideration of the Intelligence Reform Act of 2004, the Under Secretary of Defense for Intelligence established a working group to assess open source efforts throughout DOD. The effort resulted in the establishment of the Defense Open Source Council. The Council was tasked with establishing open source requirements and developing an open source strategy for all DOD components. In July 2005 there was a conference between FBIS (which would shortly merge into the National Open Source Center) and DOD open source officials. The conference aimed to improve support to military users, encourage information sharing, and inaugurate a long-term mutually beneficial relationship. However, many of the conference attendees reportedly concluded that open source collection is poorly funded, and the personnel involved in DOD open

---

[43] See Richard E. Rowberg, "Commercial Remote Sensing by Satellite: Status and Issues," CRS Report RL31218.

[44] Special efforts are taken in some cases to avoid too many hits on certain websites from computers recognizable as coming from .gov addresses.

[45] See David A. Reese, "50 Years fo Excellence: ASD Forges Ahead as the Army's Premier OSINT Unit in the Pacific," *Military Intelligence Professional Bulletin*, October-December 2005.

source efforts often lack training in media analysis and foreign language capabilities. Furthermore, it was concluded that "there is no clear external point of contact or central responsibility for [open source] support for the military."[46]

Although there is greater coordination between the NOSC and DOD offices in acquiring materials to reduce duplication, it is not clear that the inherent challenges in training intelligence personnel in open source collection and analysis have been eliminated. Although information is shared more extensively and certain open source functions have been rationalized,[47] the open source efforts are in large measure are conducted in isolation from the NOSC and even other DOD entities.

In the FY2006 the Defense Authorization Act Congress found that the Intelligence Community "has not expanded its exploitation efforts and systems to produce open-source intelligence," and directed DOD to prepare a plan for funding a "robust" open source intelligence capability under the oversight of the Under Secretary of Defense for Intelligence.[48] The legislation also mandated plans for incorporating an open source intelligence speciality into military personnel systems and for using reserve personnel to support the open source intelligence mission.

Department of Homeland Security (DHS)

DHS, which is by statute both an intelligence and a law enforcement agency, is an important consumer of open source information and potentially able to make far more extensive use of it given the disparate extent of DHS responsibilities. Currently, DHS is focusing its open source effort on working in cooperation with state and local entities. The goal is to establish open source collection with in the various component agencies of DHS, relying on the Open Source Center for technical support and training.

Charles Allen, the Assistant Secretary for Intelligence and Analysis of DHS testified in May 2006:

> We're looking at putting together a cadre of governmental specialists, as well as contractors from my office, to work as a virtual satellite bureau of the open-source center that is run by the CIA to ensure that we meet the requirements not only of the federal government for homeland security open-source information but that we also make available this information and we push it down to the states. The states also . . . have open-source things publicly and lawfully acquired that we hope to have pushed back to us.[49]

---

[46] Douglas Peak, "DOD and the DNI Open Source Center — Building the Partnership," *Military Intelligence Professional Bulletin*, October-December 2005, p. 16.

[47] For instance, the headlines of the leading Chinese military newspaper are now summarized by the Open Source Center rather that the ASD, freeing up resources in the latter. Ibid., p. 17.

[48] P.L. 109-163, section 931.

[49] Federal News Service, Testimony of Charles Allen, Assistant Secretary, Department of Homeland Security to House Homeland Security Committee, May 24, 2006.

Open source acquisition and use at DHS appears to be in the formative stages, a situation similar to that existing at many agencies. There is an acceptance of the need for greater use, but the infrastructure is incomplete and observers believe that full utilization of available sources has not been obtained.

Metrics for Open Source Use

One of the key challenges to managing the use of open source is the absence of widely accepted measurements or metrics. Intelligence Community managers seek quantifable measures for day-to-day administration. Counts are made of the occasions in which open source analyses have been included in the President's Daily Brief, one of the Intelligence Community's most important products. Other products are published by the Open Source Center based solely on open source information and disseminated to intelligence analysts and outside experts. Use of the website *opensource.gov* is also monitored.

Inasmuch as open source information is used by all-source analysts in connection with information from classified sources, it is difficult to measure how much open source information contributes to a specific intelligence product. It is anticipated that open source information will increasingly be relied upon given its greater availability, the nature of issues that today's analysts must cover, and the heavier emphasis placed on it by senior intelligence leaders. The ultimate metric for the Intelligence Community is, however, the quality of analysis. Today's analysts work with the awareness that products reflecting ignorance of information contained in open sources will discredit the entire intelligence effort. This will be especially the case when intelligence products are made public and are scrutinized by knowledgeable outside experts.

Congressional Oversight of Open Source: Potential Options

Congress has been an important advocate of greater use of open source information; as noted above, it created a statutory requirement for increased use of open source information. In addition to ongoing oversight, some observers suggest that there are also a number of specific issues that Congress might address to further the goal of its greater use. These issues include:

- Identifying open source activities
- Copyright issues
- Moving the NOSC to the Office of the DNI

Identifying Open Source Activities

It is not clear that there are adequate reporting mechanisms to allow Congress to evaluate the implementation of mandated open source efforts. This creates uncertainties about how the mandate is progressing. For example, while the DNI currently has the statutory authority to ensure the effective execution of the budget,

including open source activities, throughout the Intelligence Community[50], the reality is that funding allocations may be affected by requirements imposed by agency heads including the DCIA. Some observers suggest that open source positions and budgets need to be effectively "fenced," or protected, to ensure that congressional mandates are implemented. This concern has been expressed in regard to open source efforts in the various agencies and even to the NOSC itself. The extent to which different priorities of CIA managerial officials and the NOSC leadership have complicated open source efforts is unknown, but oversight committees may wish to verify the current IC approach is adequately implementing the congressional open source mandate.

One way is to examine specific budget areas in which spending on open source currently can be identified. First, there are amounts indicated in budget submissions for the staff of the Deputy DNI for Open Source and, within the budget submission for the CIA, for the personnel and operations of the Open Source Center. Similar information for open source efforts in other agencies may be more difficult to identify. It is not known if relevant detailed budget information on open source efforts is included in the classified budget justification books that are presented annually to the intelligence and appropriations committees. A requirement that a Congressional Budget Justification Book (CBJB) be submitted specifically devoted to open source could provide detailed insights into open source operations and capabilities throughout the Intelligence Community. An open source CBJB would provide the information base on which more detailed open source oversight could be exercised.

Another opportunity occurs when the DNI submits to congressional intelligence committees an annual report reviewing analytical products. Arguably, these annual reports should address the use of open source information. However, oversight committees could ask for additional information on open source utilization if needed. And finally, an approach that might be considered in some situations would be a request for an alternative analysis of a specified topic solely based on open sources in order to compare it with all-source analyses. The Intelligence Reform Act specifically provided for alternative analyses[51] and, in some cases, it might be appropriate to have alternate analyses based solely on information in the public record. Such an effort could demonstrate the additive value of specific forms of classified information. If a product based on open sources was essentially consistent with an analogous analytical product based on classified sources, then the former would have the useful advantage of being more easily provided to Congress and the public.

Copyright Issues

A difficult issue for those responsible for acquiring, analyzing, and disseminating open source information within the Government is the extent to which such activities can be carried out in accordance with the provisions of laws governing

---

[50] 118 Stat. 3645.

[51] P.L. 108-458, section 1017.

copyrights. Much of the open source information acquired by intelligence agencies is in the "public domain," i.e. information for which no copyright is claimed. In other cases, as with certain commercial databases, rights to the information have been obtained by contract in accordance with usual government procurement procedures. In many other cases, however, agencies acquire copyright information without the authorization of the copyright holder (as of course millions of writers and researchers also routinely do).

In using such copyrighted information, intelligence agencies, like other users of public information, are governed by the doctrine of "fair use" (based on common law and codified in the Copyright Act of 1976 (17 USC 107)). "Fair use" permits the use of copyrighted materials without authorization from the copyright holder if certain criteria are met; these include variables such as (1) the amount and character of the use; (2) the nature of the copyrighted work; (3) the amount copied in relation to the whole copyrighted work; and (4) the effect of copying on the potential market for the copyrighted work.[52] Copyright, however, has to be claimed and defended by the copyright holder and some, if not many, would see no benefit in suing the Federal Government on such grounds. Further complications arise in regard to works published in foreign countries whose governments may or may not adhere to the Berne Convention for the Protection of Literary and Artistic Works which provides international protections for copyrighted material. A detailed analysis of the implications of copyright law on the open source intelligence effort lies beyond the scope of this Report, but it is clear that the Intelligence Community's desire to "buy it once and only once" may be in conflict with the goal of copyright holders to ensure that payment for the use of their products by multiple government agencies is not avoided.

Some may argue that Congress should consider an amendment to copyright law that would cover the open source efforts of intelligence agencies. Removing uncertainty of the extent of copyright would facilitate open source efforts and facilitate the widest possible use of the information by public officials. On the other hand, such an initiative could infringe upon the legitimate rights of copyright holders including the profits they could reasonably expect from copies sold to the many government offices.

Moving the NOSC from the CIA to the Office of the DNI

Some have proposed making the Open Source Center a component of the Office of the Director of National Intelligence (ODNI) while essentially retaining its current roles and missions. This approach would attempt to guarantee that open source resources would be managed by practitioners with significant expertise that could not be redirected for a single agency's temporary higher priority. Given the availability of information systems that extend throughout the Intelligence Community, an Open Source Center directly under the DNI arguably could meet the needs of analysts at all levels even if it had no agency homebase.

---

[52] Douglas Reid Weimer, "The Copyright Doctrine of Fair Use and the Internet: Case Law," CRS Report RL30495, pp.1-2.

The advantage of placing the NOSC directly under the DNI would be to enhance the prestige of the open source discipline by raising its profile, fencing the funding, and ensuring its independence from shifting priorities within the CIA where human intelligence collection inevitably makes heavy and continuing demands on senior officials. As part of the ODNI, the NOSC would have more visability and arguably would be better positioned to influence the use of open source throughout the Community. A disadvantage would be the need to establish an administrative infrastructure that would to some extent duplicate that which already exists within the CIA.

Placing the NOSC within the ODNI could also facilitate the NOSC's ability to support law enforcement agencies and state, local, and tribal entities. As part of the CIA, the NOSC is constrained in collecting information that will be used for law enforcement purposes in accordance with the provisions of the National Security Act precluding CIA involvement in law enforcement activities.[53] The Intelligence Community as a whole contains, however, several intelligence agencies — the FBI and DHS — that are also law enforcement agencies and use open source information to carry out their statutory responsibilities. Arguably, placing the NOSC in the ODNI would facilitate its ability to support law enforcement agencies. For instance, collecting media accounts in foreign publications or websites that provide information about potential terrorist activities that involve persons physically present in the U.S. could arguably infringe on the statutory prohibition of CIA involvement in law enforcement functions.[54]

Alternate Approaches

Congress also has broader reaching options. The Bush Administration's approach to open source intelligence is based on establishing standards and best practices at the National Open Source Center, and encouraging through various means, greater acquisition and use of open source information by analysts in all agencies. Although there has been little opposition to this approach expressed by Members of Congress, some outside observers have advocated alternative approaches.

A more radical, approach would be to establish an Open Source Agency completely outside the Intelligence Community (in addition to the existing Open Source Center). The goal would be to provide open source information not just to intelligence analysts but to all elements of the Federal Government including congressional committees. It is envisioned that the new agency would be an independent Federal agency under the Secretary of State (and similar to the Broadcasting Board of Governors). Such an entity could also be established in the Defense Department (outside of intelligence agencies) with special responsibilities

---

[53] 50 USC 403-3(d)(1): the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions."

[54] 50 USC 403-3(d)(1).

for supporting multilateral operations involving a number of countries some of whom might not be intelligence partners of the United States.

This initiative could be based on an assessment that open source information, systematically collected and analyzed, is important for all government efforts including those that cannot realistically be supported by the Intelligence Community. A particular advantage cited by advocates is that open source intelligence could support the conduct of U.S. public diplomacy efforts without what is considered the taint of the "secret world." In addition, there might be less concern about acquiring public information that included references to U.S. persons, than about intelligence agencies collecting information from all sources that included references to U.S. persons.

Proponents of this plan argue that open source information is essential for virtually all governmental functions but that the explosion of available information has not been matched by concerted efforts to acquire and analyze it. The goal would be to establish a center of expertise for the entire Federal Government and to make available to the public free universal access to all unclassified information acquired through this initiative.

At present, information provided by the NOSC is available to all government agencies, but it is designed to support the Intelligence Community. Some ask why shouldn't an "information collection and analysis" agency be established to deal with policy issues that may be of concern to other government agencies including those responsible for domestic issues? Such an effort would have to be justified on the basis of a widely perceived need and pervasive support throughout the Federal Government. This support, it seems, is not yet apparent, but advocates of a wider effort to acquire and analyze open source information may continue to make the case that it is needed to meet ongoing and emerging policy issues. It is also possible that the NOSC will become more useful as times goes on, and that its contribution will be so widely recognized that it will become a model for a larger entity that can serve all Federal organizations.

Summary

Although unclassified information has often been slighted by the Intelligence Community, a consensus now exists that open source information must be systematically collected and in fact constitutes an essential component of analytical products. This has been recognized by various commissions and by Congress in statutory language. Responding to legislative direction, the Intelligence Community has established the position of Assistant Director of National Intelligence for Open Source and the National Open Source Center. The goal is not only to perform open source acquisition and analysis functions; but also, to create a center of excellence in open source collection and analysis that will support and encourage all agencies in the Intelligence Community in the effective use of open source. The challenge is to deploy all available information sources and technologies, including cutting edge approaches, to obtain and analyze information of national security importance that is available openly.

The effort has been only underway since late 2005 but the NOSC is up and running, and providing support, including training, to open source professionals throughout the Intelligence Community. It is less clear that administrative mechanisms are in place to ensure that there is a comprehensive community-wide open source effort. It appears to observers that not all agencies have as yet made comprehensive commitments to acquiring and using open source information, nor that the ODNI has taken sufficient steps to ensure that open sources are fully exploited. Observers suggest that congressional oversight of the open source process might provide insight into current progress of Administration efforts as well as identify areas that need modification. A particular focus of congressional interest might be potential tradeoffs between classified and open source collection to ensure that needed information is obtained in the best and most cost-effective manner. The goal would be to ensure that vulnerable human agents and expensive surveillance systems are focused on obtaining information that is being actively hidden and obtainable through no other means.

Appendix: Open Source Case Study: India's 1998 Nuclear Tests

"Senator, we didn't have a clue."[55] (Response by former Director of Central Intelligence Director George Tenet in a telephone conversation with Chairman Richard Shelby in the aftermath of India's 1998 nuclear tests.)

On May 11, 1998, the Indian Government tested three nuclear devices, the first such tests in 20 years. The tests caught the U.S. Intelligence Committee by surprise. Then-Director of Central Intelligence George Tenet appointed former Admiral David Jeremiah to "examine how and why we had missed the boat so badly."[56]

In conducting his review, Jeremiah touched on a number of issues, including the availability at the time of open source information in the form of public statements made by Bharatiya Janata Party (BJP) leaders prior to the election of party leader Atal Behari Vajpayee to be India's prime minister. Those public statements indicated that the BJP was interested in exercising the nuclear option.[57]

In his final report, Jeremiah concluded:

> ...that both the intelligence and the policy communities had an underlying mindset going into these tests that the BJP would behave as we behave. For instance, there is an assumption that the BJP platform would mirror Western political platforms. In other words, a politician is going to say something in his political platform leading up to the elections, but not necessarily follow through on the platform once he takes office and is exposed to the immensity of his problem. The BJP was dead serious...[58]

Others were more explicit in their criticism. Former U.S. Senator Patrick Moynihan reportedly commented, "It didn't take spies or spy-masters simply to read what Indian leaders said and to take it seriously."[59]

These and other observations suggest that if analysts had paid greater attention and attached more significance to some of the BJP's public statements about nuclear

---

[55] George Tenet, "At the Center of the Storm: My Years at the CIA," HarperCollins Publishers (New York), 2007, p. 44.

[56] George Tenet, "At the Center of the Storm: My Years at the CIA," HarperCollins Publishers (New York), 2007, p. 44.

[57] George Perkovich, "India's Nuclear Bomb," University of California Press (Berkeley), 1999, p. 405. Perkovich's book is viewed by specialists as offering the definitive, publicly available analysis of what occurred during the lead up to India's 1998 nuclear tests.

[58] See Jeremiah News Conference, June 2, 1998.

[59] Amy Sands, "Integrating Open Sources into Transnational Threat Assessments," in Jennifer E. Sims and Burton Gerber, *Transforming U.S. Intelligence* (Washington: Georgetown University Press, 2005), p. 66.

testing, the Intelligence Community might have more accurately assessed BJP intentions.

A review of the public record prior to the Indian tests, however, presents a mixed picture in this regard and arguably underscores some of the difficulties analysts confront when attempting to analyze open source information.

During the election campaign in January 1998, the BJP's foreign policy spokesman stated that his party had every intention of exercising the nuclear option if elected.[60] But in February of that year the BJP issued a campaign manifesto that suggested to some Indian analysts that the BJP might not be fully committed to conducting nuclear tests.[61] New BJP Prime Minister Vajpayee, while reportedly stating that government would keep open the option of adding a nuclear capability to its arsenal, said there was no time frame for doing so.[62] The government's defense minister further suggested there was no need to test nuclear weapons.[63]

Amid other public signs that included no indication of imminent nuclear testing, a high-level U.S. delegation met with their Indian counterparts and concluded that no such tests were imminent.

In the final analysis, open source information that was available prior to India's nuclear tests in 1998 presents a mixed if not misleading picture that presented a number of analytic challenges.

---

[60] George Perkovich, "India's Nuclear Bomb, University of California Press (Berkeley), 1999, p. 405.

[61] Ibid, p. 407.

[62] Ibid, p. 408.

[63] Ibid, p. 408.