Open Source Intelligence (OSINT)

Greg S. Weaver

Intelligence is a process as well as a product, the end result of transforming information into knowledge (Peterson, 2005). This statement also applies to open source intelligence (OSINT). Open source intelligence includes the synthesis of information available from outlets accessible to the public. Important examples of relevant information include that which is obtained from media outlets, publicly available documents and data, the Internet, professional and/or academic reports, articles, books, and "grey literature" which refers to academic and professional reports that are more difficult (but not impossible) to obtain from public outlets (Jardines, 2002; Lowenthal, 2003; Soule & Ryan, 2002). The terms *information* and *intelligence* are often used interchangeably when describing that which is obtained from open sources, but there are important differences. Just as putting flour, eggs, milk, sugar, etc., into an oven does not automatically result in a cake, open source data and information must be turned into open source intelligence. OSINT results when analysis and research is applied to open source information (Peterson, 2005). However, the utility of intelligence, including OSINT, cannot be realized unless it is also disseminated to those agencies that need it (Gunaratna & Chalk, 2002).

A North Atlantic Treaty Organization (2001:2-3) review outlines a taxonomy that shows how information and intelligence are not one in the same. In making this distinction, NATO identifies four primary categories, with subsequent categories building upon the previous one(s):

Open Source Data
⬇
Open Source Information
⬇
Open Source Intelligence (OSINT)
⬇
Validated OSINT

Open source data consists of the plethora of raw materials that may be obtained from one or more sources, including oral and printed communication and/or documents as well as visual information (e.g., maps, photographs, and satellite images). Data that have been compiled and broadly organized constitute *open source information*. Open source Information has been subjected to a limited level of review and validation. Upon further analysis, open source information may be condensed, synthesized, and verified to produce open source intelligence. OSINT is usually distributed to a restricted and selected audience. The final category – Validated OSINT – consists of the final product that has been subjected to further verification/validation, often with corroborating evidence obtained from sensitive or closed sources. The repeated "distillation" and validation increases the accuracy and utility of the finished product. In that respect, OSINT can then be utilized by the collecting agency and others as a tool for a number of tasks.

OSINT is a valuable resource, but in some ways it can be a "double-edged sword" in that its benefits are also liabilities. A primary advantage of OSINT is that it is widely available from a number of sources. Because of few (if any) restrictions on use and distribution, open source information can be rapidly collected and, depending on the extensiveness of the accompanying

analysis performed, communicated or forwarded to others (Lowenthal, 2003; NATO, 2001). On the other hand, the sheer volume of available data and information can prove to be an impediment (Lowenthal, 2003). Identifying the relevant piece(s) from such a large body of data/information is a daunting task indeed. Vast amounts of data are difficult to organize and process, and the quality of some sources is suspect (Soule and Ryan, 2002).

One pertinent example of this issue can be found in information obtained from online sources. The Internet is becoming an increasingly important channel for obtaining open source information. However, the validity of some Web-pages or of documents contained in them is at best questionable. Some sources may contain inaccurate, biased, or misleading (unintentional or intentional) information. Also, documents and sites may be removed entirely from the Web, making it necessary to regularly archive entire Internet pages (Jardines, 2002). Another confounding issue is known as *echo*, when unsubstantiated information contained in one source is cited (without verification) by another. As a result, the relevance of a piece of inaccurate or unverified information may be exaggerated if it is reported in multiple outlets.

The amount of available information has increased exponentially, but development of actionable intelligence from it has not occurred at a similar pace (Lowenthal, 2003). While the military and law enforcement at all levels are under increasing pressure to develop and enhance intelligence capabilities, Peters (2006) warns that intelligence is not a panacea, suggesting that unrealistic expectations on the part of the public, agencies, and politicians alike must be tempered. Intelligence is but one of many tools that can be employed, but it does not replace the human element.

In the United States, the bulk of information contained in intelligence documents comes from open sources. OSINT is particularly valuable when coupled with other forms of intelligence or restricted materials. The latter (sensitive or classified information) is value added to the context and framework provided by the OSINT (deBorchgrave, Sanderson, and MacGriffin, 2006; Johnson, 2003). OSINT is a key piece of the figurative intelligence puzzle, yet its importance is often understated by the intelligence community (IC) itself (deBorchgrave et al., 2006). As mentioned elsewhere, the nature of crime is changing in important ways including that some activities transcend jurisdictional and geographical boundaries. Therefore, the responses to them must also be adjusted. In some ways, the use and sharing of OSINT is a possible mechanism through which cooperation between agencies and departments, laterally and vertically, can be improved.

The traditional IC is viewed as having a preventive or proactive function, whereas law enforcement has a greater reactive or investigative role. These different but complementary missions have, no doubt, affected the respective cultures of each. An unintended and unfortunate consequence is the lack of trust between agencies (Office of the Director of National Intelligence, 2005; 2007).

In some ways, intelligence as a process and as a product is viewed as a function of national security interests, not law enforcement. The former is designed to prevent harm and to protect the interests of the country, whereas law enforcement agencies have traditionally fulfilled an investigative role (Markle Foundation, 2003). The distinction of two categories of intelligence, tactical and

strategic, assists in illustrating this issue. Tactical intelligence refers to that which is typically associated with a particular case or investigation. In many instances, this intelligence may be archived or stored upon completion of an investigation, but it is usually not re-examined in the context of the larger law enforcement mission. Strategic intelligence, on the other hand, is more closely associated with the proactive elements of intelligence, focusing on the "big picture," as opposed to a specific incident or case (Best, 2001; Peterson, 2005). The following example related to drug trafficking illustrates this distinction. Strategic intelligence would include knowledge about trafficking organizations, methods, and routes, whereas information on a specific shipment illustrates tactical intelligence (Best, 2001). Similarly, strategic intelligence is not limited to the enforcement function only. It is also a key component in planning efforts, staffing decisions, and in the development of policy and priorities (Evans, 2005).

However, Osborne (2006) correctly asserts that the process of taking information and, through research and analysis, producing actionable intelligence, differs little for law enforcement, intelligence agencies, or the military. This point is relevant for two key reasons. First, the boundaries between crime and issues related to national security have become increasingly blurred. For example, it is a widely held belief that proceeds from illegal drug trafficking are an important source of funds for terrorist organizations (Sullivan, 2001). Second, some acts, such as terrorism, human trafficking, and cybercrime, transcend geographical and jurisdictional boundaries. As a result, the need for cooperation between countries is increased. Deflem (2006) points to Europol as one such example. The jurisdiction and authority of Europol is defined in part by agreement between the member states of the European Union. Liaisons from one country are stationed in another. Similarly, the FBI has begun to assign attaché offices in a number of foreign countries. These arrangements not only increase the capacity to investigate crimes that cross national boundaries but also serve to provide a medium for information exchange as well as to strengthen relationships between individuals and agencies alike (Best, 2001). Studeman (2007) asserts that the intersection of different elements of the intelligence community is a function of cross-jurisdictional boundaries.

Beginning in the 1970s, an increasing number of restrictions were placed on domestic agencies in terms of having access to or collecting information on U.S. citizens unless that material was pertinent to an ongoing investigation or if reasonable suspicion warranted such action. However, these restrictions have been eased somewhat since 9/11 via changes authorized by the USA PATRIOT ACT (Markle Foundation, 2003). Clearly, the concern over compiling and accessing information on U.S. citizens is legitimate, but given that the boundaries between crime and national security have become increasingly blurred, balancing these concerns is of utmost importance. For example, since 9/11, law enforcement agencies have been allowed more leeway in terms of collecting intelligence, such as conducting public surveillance and performing Google searches (Markle Foundation, 2003). Both of these examples arguably fall under the general category of OSINT.

McNamara (2007) notes that at the present, a national, unified system for distributing unclassified information does not exist. Legal concerns and the cultures

of constituent agencies contribute to this problem. Until such a system has been developed, information sharing, laterally and vertically, will be less than optimal. A report of the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction suggests that the FBI, because of its dual role as an investigative and intelligence agency, is particularly well-suited to become the point through which intelligence is shared, provided that the long-standing practice of "stovepiping" information and a general sense of mistrust are ameliorated (Office of the Director of National Intelligence, 2005). Since 9/11, the FBI has, in fact, assumed a greater intelligence function, in part because the Bureau falls under the purview of the Office of the Director of National Intelligence. As a member of and in conjunction with the Joint Terrorism Task Force (JTTF) units established throughout the country, its potential as an information conduit to other agencies has increased (Johnson, 2003; Markle Foundation, 2003; Markle Foundation, 2006). Additionally, it is suggested that because of the law enforcement role of the FBI, the concerns over collecting information on U.S. citizens and their civil liberties will not be ignored (Office of the Director of National Intelligence, 2005).

As mentioned previously, a long-standing bias in the intelligence community is that OSINT is inferior to classified or "high side" material. Also, for a number of reasons, there has been a tendency to overclassify or to restrict the availability of intelligence. This "need to know" approach limits the distribution of material that may be of benefit to a number of agencies. It is apparent that clear guidelines are necessary to facilitate the sharing of both open source and sensitive/classified information. Just as the definition of *law enforcement sensitive* differs across jurisdictions and agencies, so, too, does the question over who can have access to this information (Markle Foundation, 2003; McNamara, 2007). It has been suggested that an important change lies in moving from a philosophy of "need to know" to one of "responsibility to provide" information to those agencies that need it (Office of the Director of National Intelligence, 2007).

Another step in addressing these concerns lies in increasing the use of and access to OSINT. The Markle Foundation (2003) recommends that the emphasis should be placed on creating distributable products whose access can be restricted as more sensitive or even classified information is added, as opposed to automatically restricting this information at the onset. The dissemination of OSINT can be regulated via guidelines established beforehand, so development of consistent and usable policies is important. For example, the use of a virtual private network (VPN) dedicated to OSINT could greatly enhance the intelligence capabilities of various agencies and departments. Because the information contained in them is not classified per se, it is not necessary to hold a security clearance in order to access it.

Conclusion: "Where do we go from here?"

Clearly, a number of challenges must be addressed in order to better use OSINT. However, it accomplishes little to lament what has not been done in the past or to recommend unrealistic measures that are not feasible within the existing intelligence system. Perhaps one way to move forward is to acknowledge and learn from mistakes of the past. The following discussion takes this approach.

In *Sharing the Secrets: Open Source Intelligence and the War on Drugs*, Holden-Rhodes (1997) offers a compelling, yet controversial, account of how "round five (p. 2)" of the War on Drugs beginning in the 1980s was hindered by a lack of coordination, cooperation, and information sharing between various departments, agencies, and the military. The alleged under-utilization of OSINT is central to these claims. For example, Holden-Rhodes contends that OSINT can provide valuable information on drug trafficking and distribution.

In Holden-Rhodes opinion, one of the factors contributing to the failure of the War on Drugs occurred years earlier. From 1969-74, the Nixon administration characterized anti-drug efforts as an issue of national security. However, local, state, and federal law enforcement agencies have a prominent role in domestic drug issues, and its relationship vis-a-vis the military is complex. Poorly defined goals and unrealistic expectations led to political wrangling in a number of areas, and policy suffered. During the 1980s and beyond, the emphasis on anti-drug efforts resulted in large increases in available funding. According to Turner (1999), various agencies and departments scrambled to secure their share of the figurative financial pie. This competition resulted in a lack of cooperation between agencies, both horizontally (federal) and vertically (federal-state-local).

The "national security versus crime" debate is apparent in terrorism policy as well (for a recent review, see LaFree & Hendrickson (2007)), and there is no dearth of compelling arguments in support of either position. A detailed discussion is not needed to recognize that at times, the similarities between the war on drugs and the developing policies related to the global war on terror are unnerving. In essence, the author argues that the War on Drugs has been ineffective in large part because a rational, unified strategy is lacking. Furthermore, without a clearly defined system of command and control, the objectives at hand can be lost. He agrees with Wilson (1983, p. 49) who asserts that a rational policy must clearly identify goals and objectives and be geared to recognize the ones that are attainable (and those that are not) and what level of influence the government has to manipulate those goals or conditions to achieve the desired results. In short, the "Global War on Terror" falls on the collective shoulders of a number of agencies and departments, and cooperation is of utmost importance.

REFERENCES

Best, R. A., Jr. (2001). *Intelligence and law enforcement: Countering transnational threats to the U.S.* (CRS Report for Congress #RL30252). Washington, D.C.: Congressional Research Service.

deBorchgrave, A., Sanderson, T., & MacGaffin, J. (2006). *Open source information: The missing dimension of intelligence* (Report of the CSIS Transnational Threats Project). Washington, D.C.: CSIS Press.

Deflem, M. (2006). Europol and the policing of international terrorism: Counter-terrorism in a global perspective. *Justice Quarterly*, *23*, 336–359.

Evans, S. (2005). Law enforcement and Delphi: An exercise in strategic intelligence research. *Low Intensity Conflict & Law Enforcement*, *13*, 70–79.

Gunaratna, R., & Chalk, P. (2002). *Jane's counter terrorism* (2nd ed.). Surrey, U.K.: Jane's Information Group.

Holden-Rhodes, J. F. (1997). *Sharing the secrets: Open source intelligence and the war on drugs*. Westport, CT: Praeger.

Jardines, E. A. (2002). *Theory and* history *of OSINT: Understanding open sources*. Retrieved July 15, 2007, from http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf.

Johnson, L. K. (2003). Bricks and mortar for a theory of intelligence. Comparative *Strategy*, 22, 1–28.

LaFree, G., & Hendrickson, J. (2007). Build a criminal justice policy for terrorism. *Criminology and Public Policy*, 6, 781–790.

Lowenthal, M. M. (2003). *Intelligence:* From *secrets to* p*olicy* (2nd ed.). Washington, D.C.: CQ Press.

Markle Foundation Task Force. (2003*).* Creating *a trusted network for homeland security* (Second Report of the Markle Foundation Task Force). New York: Markle Foundation. Retrieved July 8, 2007, from http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf.

Markle Foundation Task Force. (2003). *Mobilizing information to prevent* terrorism*: Accelerating development of a trusted information sharing environment* (Third Report of the Markle Foundation Task Force). New York: Markle Foundation. Retrieved July 8, 2007, from http://www.markle.org/downloadable_assets/2006_nstf_report3.pdf.

North Atlantic Treaty Organization. (2001). *NATO open source intelligence handbook*. Retrieved July 15, 2007, from http://www.oss.net/dynamaster/file_archive/030201/ca5fb66734f540fbb4f8f6ef759b258c/NATO%20OSINT%20Handbook%20v1.2%20-%20Jan%202002.pdf.

Office of the Director of National Intelligence. (2005). *The commission on the intelligence* capabilities *of the United States regarding weapons of mass destruction* (Report to the President of the United States). Washington, D.C.: Program Manager, Information Sharing Environment. Retrieved July 15, 2007, from http://www.ise.gov/docs/wmd%20report.pdf.

Office of the Director of National Intelligence. (2005). *The national counterintelligence strategy of the United States of America* (Report to the President of the United States). Washington, D.C.: Program Manager, Information Sharing Environment. Retrieved July 15, 2007, from http://www.dni.gov/reports/NCIX_Strategy_2007.pdf.

Osborne, D. (2006). *Out of bounds: Innovation and change in law* enforcement *intelligence analysis*. Washington, D.C.: JMIC Press.

Peterson, M. (2005). *Intelligence-led policing: The new intelligence architecture* (NCJ 210681). Washington, D.C.: United States Department of Justice.

Soule, M. H., & Ryan, R. P. (2002). *Grey* literature. Retrieved July 15, 2007, from http://www.oss.net/dynamaster/file_archive/030201/254633082e785f8fe44f546bf5c9f1ed/NATO%20OSINT%20Reader%20FINAL%2011OCT02.pdf.

Studeman, M. W. (2007). Strengthening the shield: U.S. Homeland Security *Intelligence*. *International Journal of Intelligence and Counterintelligence*, *20*, 195–216.

Sullivan, J. P. (2001). Gangs, hooligans, and anarchists: The vanguard of netwar in *the* streets. In J. Arquilla & D. Ronfeldt (Eds.), *Networks and*

netwars: The future of terror, crime, and militancy (pp. 99–127). Santa Monica, CA: Rand Reports. Retrieved July 23, 2007, from http://www.rand.org/pubs/monograph_reports/MR1382/MR1382.ch4.pdf.

Turner, M. A. (1999). Open sourcing the drug war. *International Journal of* Intelligence *and Counterintelligence*, *12*, 103–108.

Wilson, J. Q. (1983). *Thinking about crime* (Rev. Ed.). New York: Vintage Books.