CSS Analyses in Security Policy

CSS ETH Zurich

Vol. 3 • No. 32 • April 2008

OPEN SOURCE INTELLIGENCE: A STRATEGIC ENABLER OF NATIONAL SECURITY

The importance of Open Source Intelligence (OSINT) has grown in recent years. For the traditional intelligence community, OSINT is likely to remain one component of an all-source intelligence capacity that includes classified sources. For most government agencies, however, OSINT is the only intelligence they have access to, which renders it a strategic enabler of decision- and policy-making. Governments should consider formulating a national OSINT strategy and establishing an OSINT center to allow for the effective exploitation of open source information.

www.istockphoto.com

Open Source Intelligence (OSINT) has gained considerable prominence in recent years. Traditionally, intelligence has been the business of discovering secrets using a closed system of collection and analysis. Key sources included human intelligence (HUMINT), signals intelligence (SIGINT), and imagery intelligence (IMINT). Although open sources were frequently used in the intelligence process, their value was seen as secondary. Classified information was deemed more valuable and often more credible. The systematic acquisition of non-classified information was rarely seen as an intelligence priority.

Today, OSINT's importance is widely acknowledged. It is estimated that OSINT provides between 80 and 95 per cent of the information used by the intelligence community. There is a growing debate within and between the various branches of government and the national security apparatus on how best to use open source information. However, the role and potential of OSINT remain a matter of some dispute. OSINT's advocates believe it to be the answer to many of today's intelligence challenges. They call for a new intelligence paradigm marked by a preponderance of open source information and a trans-sector intelligence collaboration that includes a broad network of public and private actors. But there are others who warn against treating OSINT as more than a component of a continuing, all-source approach to intelligence-gathering and analysis.

OSINT drivers

In order to understand the OSINT debate, it is useful to first define the concept. OSINT is information gathered from publicly available sources for the purpose of meeting specific intelligence requirements. These sources can be free or subscription-based, on- or offline. OSINT is not limited to the internet, although it is here that an increasing volume of valuable information is to be found. The media, public agencies, think-tanks, universities, NGOs, and the private sector all constitute open sources of information.

The evolution of the OSINT debate can be attributed to three main factors. The first is the broadening of the security agenda over the past two decades. During the Cold War, intelligence services were preoccupied with a limited number of largely state-centric challenges. Discovering the intentions and capabilities of the Soviet Union was the primary task of the Western intelligence community. Since the fall of the Berlin Wall, however, these threats have multiplied and become more diverse in terms of their agents and nature.

Accordingly, the range of issues that intelligence agencies are required to deal with has widened dramatically. Today, these include, inter alia, terrorism, the proliferation of weapons of mass destruction, organized crime, fragile states, intra-state conflict, illegal immigration, and energy security. Since the attacks in the US on 11 September 2001, many government agencies have had to contend with the securitization of their core concerns, whether they be transport, food, water, or the environment. The broadening of the security agenda has raised the demand for more information, which in turn has fostered a growing appreciation of the value and utility of OSINT.

A second driver is technology. The evolution of the internet and the emergence of the collaborative web have alerted security actors to the potential of new tools and technologies for collecting, analyzing, and distributing knowledge on global affairs. The proliferation of websites, portals, wikis, and blogs has opened a world of information hitherto unavailable to most intelligence professionals.

Google Earth provides more geospatial intelligence than was available to most governments less than a decade ago. Even services such as Wikipedia are increasingly cited as intelligence sources. There is also a growing market for commercial intelligence vendors offering products and services previously restricted to the public sector. Thanks to the information revolution, the traditional intelligence community no longer has a monopoly on the skills or information needed to understand, analyze, or address today's security threats.

The intelligence failures surrounding 11 September 2001 and the invasion of Iraq have also driven this development. Particularly in the US, these failures have prompted a thorough reassessment of the way in which intelligence is used to shape the policymaking process. After successive commissions stressed a need for the intelligence community to make greater use of OSINT (if only to verify the opinions and conclusions of classified sources), an Open Source Center was established by the US Director of National Intelligence in November 2005. Since then, the number of OSINT positions in the US intelligence community has grown. The OSINT debate has also intensified in other countries, particularly in Europe.

OSINT benefits

OSINT advocates are keen to highlight its benefits. Perhaps the most immediate of these is the issue of cost. OSINT is considerably less expensive than collecting information via classified means. Researchers and journalists working in the field, for example, are a valuable source of human intelligence. Helpful communications intelligence can be found on the many blogs and forums dedicated to international affairs, as well as in the letters pages of every quality newspaper. High-quality imagery intelligence is freely available from Google Earth and similar services. The fact that OSINT offers a potentially greater return on investment than satellites and other classified sources is particularly relevant for countries operating on tight intelligence budgets.

Open source intelligence also has other major advantages. To begin with, it is shareable. Information collected by one organization can be given to another at little or no cost. Second, OSINT collected using ethical means can be used in legal proceedings without risking the exposure of sensitive intelligence assets. Indeed, OSINT constitutes almost zero risk compared to intelligence operations using spies and other clandestine assets. Third, OSINT can be accessed, exploited, and shared around the clock. And fourth, intelligence gathered from authoritative public sources can be used to inform the public of serious threats to national security.

Open source information: Useful sites

The following websites provide a wealth of open source information for researchers and analysts interested in global affairs:

- International Relations and Security Network (www.isn.ethz.ch)
  Based at the Center for Security Studies at the Swiss Federal Institute of Technology (ETH Zurich), the ISN collects and manages resources from hundreds of different think-tanks, research institutes, international organizations, and government agencies in its digital library. It also publishes a daily news analysis service, Security Watch, and indexes the content of thousands of IR- and security-relevant websites.
- Oxford Analytica (www.oxan.com)
  A premium rate strategic analysis and consulting service drawing on a network of university researchers and faculty members at Oxford and other major universities around the world.
- Newstin (www.newstin.com)
  An innovative news aggregation service that pulls content from thousands of different media sources from across the globe. Newstin's language translation features also allow visitors to read information published by foreign news and information sources at the click of a button.

Finally, and perhaps most important of all, OSINT provides context and awareness that is critical to an understanding of the global security agenda. The growing complexity and interconnectedness of our world, and the declining degree of certainty and predictability, have underlined the importance of horizon scanning and long-term strategic intelligence assessments that draw on the knowledge of multiple sources and disciplines.

Limitations and weaknesses

OSINT is not without its limitations. For traditional intelligence agencies, it is unlikely to offer a 100 per cent solution to their information needs. Indeed, it is only likely to compound the problems they already face, the greatest of which is information overload. Filtering the "signals" from the "noise" is becoming increasingly difficult and time-consuming. The promises made by technology vendors, no matter how sincere, cannot replace the enormous analytical effort that the wealth of OSINT requires from human beings.

Furthermore, the fact that multiple news agencies report an event may not make it accurate or true per se. Governments and non-state actors are just as likely to use open sources of information to broadcast inaccurate or misleading information. On occasion, OSINT needs to be verified against information from classified sources.

The usefulness of OSINT does not always extend to providing actionable intelligence on the tactical or operational level. While it may provide a rich source of information on the grievances and motivations of al-Qaida, OSINT will not necessarily reveal the exact location of Osama bin Laden or the tactical information needed to capture him. As militant groups and organized crime syndicates become aware of just how large their "digital footprint" really is, they are more likely to go offline and stay below the radar. Similarly, while OSINT has been used to acquire intelligence on Iran's nuclear program, it cannot provide real-time insight into exchanges of information between Iranian scientists.

Tailoring OSINT to individual needs

Two conclusions can be drawn from the above assessment. First, making strategic use of OSINT is necessary, feasible, and promising. Second, OSINT will mean different things to different people. For the traditional intelligence community, OSINT is likely to remain one component of an all-source information collection capacity that includes clandestine sources. Clearly, traditional intelligence processes will need to be further refined to make better use of OSINT. For most government agencies, however, OSINT is the only "INT" they have access to. It is the source of first and only resort and a strategic enabler of policy- and decision-making.

Naturally, the challenge of promoting a more systematic use of OSINT will vary depending on the government agency in question. Within the traditional intelligence community, what is required most is a change of mindset. Many analysts, particularly those shaped by the Cold War, continue to be biased against OSINT and refuse to acknowledge its value. Indeed, information collected from open sources is routinely stamped "SECRET" and put under lock and key, thus limiting its utility. Remarkably, a number of Western intelligence agencies continue to deny their staff access to the internet on the grounds of security.

To be effective, the intelligence community will need to invest more in developing its OSINT capacities. A first step would be to improve the training given to researchers and analysts tasked with finding and exploiting open sources of information. Improving language skills is also of vital importance. The most valuable intelligence is often in a language other than the one spoken at the office. Additional IT investment is also necessary, even if it is unlikely to provide a "silver bullet" to the challenge of information overload.

Looking beyond the OSINT needs of the intelligence community, the challenge is greater still. Government players should avoid agency-specific solutions that lead to a duplication of effort and an uncoordinated system of outsourcing contracts and partnership agreements. This requires an all-government OSINT strategy that addresses some fundamental challenges: How should one build an organization capable of exploiting the collective intelligence of thousands of disparate sources? How does one break down information silos and encourage greater knowledge-sharing and collaboration? Where does one find staff capable of thinking and working across disciplines? How does one manage the rapid evolution of technology? What policies and processes can be put in place to boost operational effectiveness? None of these questions are easy to answer. Governments will need to tailor their approaches to meet the information needs of all their constituents.

The merits of an OSINT center

One way forward would be to establish a national OSINT center that is mandated to provide OSINT to all branches of the government. Such a center can be positioned within an existing national security framework or stand alone as an autonomous entity. Either way, it should remain free from the influence of any one government department.

Institutionalizing OSINT: The US model

Assistant Deputy Director of National Intelligence for Open Source

- Establishes open source strategy, policy, and program guidance
- Makes sure that a single open source architecture is developed
- Advises agencies and departments outside the National Intelligence Program regarding the acquisition of OSINT.

National Open Source Committee

- Provides guidance to the national open source enterprise
- Members are senior executives from the Open Source Center, Office of the Under Secretary of Defense for Intelligence, Department of Homeland Security, CIA, National Security Agency, National Geospatial-Intelligence Agency, Department of State's Bureau of Intelligence and Research, Defense Intelligence Agency, Federal Bureau of Investigation, Office of the intelligence community's CIO

Open Source Center

- Created in 2005 by the Director of National Intelligence, with the CIA as its executive agent
- Several hundred full-time personnel
- Advances the intelligence community's exploitation of open source material; helps to develop mini open source centers within the respective agencies
- Nurtures acquisition, procurement, analysis, dissemination, and sharing of open source information, products, and services throughout the government
- Makes reports, translations, and analytical products available online in a secure website available to government officials (www.opensource.gov)

Sources: Intelligence Community Directive No. 301; CRS Report for Congress, 5 December 2007.

A joint OSINT center could be tasked with supporting the all-source capabilities of clandestine intelligence services; track trends in IT and provide government agencies with the tools and technologies they need in order to acquire and exploit the information better; establish collaborative partnerships with non-government actors; communicate best practices in the collection, management, analysis, and dissemination of information; provide training and education to government researchers; and conduct early-warning and long-term foresight activities.

An OSINT center should combine permanent staff (information professionals, intelligence analysts, IT experts, etc.) together with rotating staff from different government agencies. In order to keep personnel costs low, it should tap knowledge and expertise from academia and the private sector as systematically as possible. While establishing and maintaining such a center will require a sizable financial investment, it is bound to save governments a considerable sum of money on an annual basis by consolidating access to premium information services and coordinating IT investments.

Switzerland and OSINT

A number of recent initiatives have illustrated the growing importance of OSINT in Switzerland. An interdepartmental OSINT Working Group has been established to explore possible synergies between various government agencies. A second working group deals with OSINT at the Federal Department of Defense, Civil Protection, and Sports. The Strategic Intelligence Service (SND) and the Military Intelligence Service (MND) have institutionalized OSINT, as has the domestic intelligence service at the Federal Police Department, where a small OSINT section was founded in 2001. Also, individual departments have bought their own information gathering systems, some of which have failed to meet expectations.

Still lacking is the formulation of a national OSINT strategy that would coordinate OSINT activities at the political level, define roles and responsibilities and, if necessary, create a centralized OSINT infrastructure for all interested departments. The current debate on a revision of the civilian intelligence agencies and the creation of a federal security department should be regarded as an opportunity to investigate and clarify the future role and institutional implementation of OSINT in Switzerland.

- Author:
  Chris Pallaris
  pallaris@sipo.gess.ethz.ch
- Responsible editor:
  Daniel Möckli
  analysen@sipo.gess.ethz.ch

- Other CSS Analyses / Mailinglist:
  www.isn.ethz.ch
- German and French versions:
  www.ssn.ethz.ch