National Intelligence and Open Source: From School House to White House
by Robert David Steele

Mr. Robert D. Steele, our Contributing Guest Editor, is President of OPEN SOURCE SOLUTIONS, Inc., a corporation chartered in the State of Virginia. On 1 April 1992 Mr. Steele resigned from his senior civilian position with the Marine Corps (he remains a Reserve officer-instructor at Marine Corps Command & Staff College, with full clearances) to devote himself full-time to open source intelligence (OSINT) issues. It was this personal initiative which led to the first International symposium on "National Security & National Competitiveness: Open Source Solutions".

Mr. Steele was named as one of the 'Microtimes 100: Industry leaders and unsung heroes who made a difference in the computer industry in 1992 and helped create the future'.

The private sector can take advantage of the over-all decline in funding for the national intelligence community by exploiting three distinct areas of need in the open source arena, where returns on investment virtually assure rapid growing demand for contractor services. As the intelligence community restructures itself and adjusts to changing fiscal and threat environments, three questions are on the minds of those committed to changing the way we do business:

• First, what multi-media data sources and products can be collected, processed, and sold by the private sector to meet government needs – in other words, how can we define and then privatize much of the government's need for open source information?

• Second, what tools, technologies, and methodologies are on the shelf or emerging which can be of significant assistance to both government and the private sector as each seeks to exploit open sources for competitive advantage – how can we cut costs by standardizing and integrating our databases, applications, and technologies?

• Third, what joint endeavors, such as cooperative agreements to digitize and share Third World scientific and technical data, can be entered into between government and the private sector (including the academy) in order to collect, process, and disseminate open source data helpful to the Nation's competitiveness?

The dark side of the restructuring within the intelligence community is clear – we will do more with less.

On the bright side, Open Source Intelligence (OSINT), once known as scholarship, journalism, or investigation, is finally coming into its own. OSINT is a good remedy for those receding analysis of threats for which our existing collection and production capabilities are unsuited; OSINT also offers a return on investment which far exceeds that of any other discipline. Finally, a commitment to OSINT, with a commensurate effort to support national education and national enterprises, offers a means by which both legislative and executive leaders can support national competitiveness without diverting or undermining classified capabilities. For these and other reasons, OSINT merits serious attention from industry.

Within the national intelligence community, while a full commitment to this discipline has yet to be articulated, there is a growing consensus that OSINT requires a substantive increase in investment. The Director of Central Intelligence (DCI) has been reputed to refer to "the four INTs" and to subsequently explain that he was referring to OSINT rather than
Measurements and Signatures Intelligence (MASINT). The DCT’s appointment of an Open Source Coordinator provides a focal point for developing a concrete and very broad program-in full partnership with our private sector-to meet the unfunded deficiencies in open source multi-media collection, processing, and dissemination.

Outside the intelligence community, under the leadership of the Administrator of the Defense Technical Information Center (DTIC), there is an extraordinary semi-official consortium called CENDI which brings together managers of scientific and technical information resources and which has much to offer as a model for inter-agency cooperation on open source issues. CENDI, together with the Open Source Coordinator, and perhaps such industrial organizations as the Information Industry Association, offers a basis for coordinating a major expansion of government investment in open source capabilities and products.

A systematic approach to OSINT as a separate discipline is the only means by which this discipline can be nurtured and managed in a declining fiscal environment. What is OSINT? The figure below reflects a personal best estimate (not hard data) of what we capture from available print, broadcast, and imagery open sources; and of what we spend on overt as opposed to other forms of collection.

Although existing intelligence community requirements and priorities processes can be considered as applicable to OSINT as they are to other disciplines, in fact there is no real channel for consolidating open source requirements and tasking open source capabilities. There has never been serious support for OSINT within the intelligence community except as narrowly defined by the Foreign Broadcast Information Service (FBIS) and other community elements focused on Soviet scientific and technical literature.

There are many analysts who will testify that their management and their culture is actively biased against the exploitation of open sources. It merits comment that it is much easier for the analyst to task classified capabilities than to obtain foreign literature, transcripts of foreign video broadcasts, or commercial imagery products. This is the case even though classified sources by definition have a narrower focus and restricted production.

---

**AlliedSignal**

**TECHNICAL SERVICES CORP.**

One Bendix Road
Columbia, Maryland 21045

**INTELLIGENT Intelligence Systems**

- ✔ Engineering
- ✔ Analysis
- ✔ Development
- ✔ Simulation

Our name has changed from Bendix Field Engineering Corp.
For more information call Peter Dachel at 800-638-6417 ext 7074
Requirements for open sources tend to be ad hoc; although there is a good understanding of community elements interested in open sources, there has never been a systematic attempt to survey and understand the open source needs of policy consumers, Service and Department planners, theater commanders, and tactical commanders. The military warfighters, at least, appear to be unanimous in lamenting the classification and handling constraints associated with Sensitive Compartmented Information (SCI) documents, and adamant that they require unclassified materials which can be shared with both uncleared troops and uncleared coalition and non-governmental organizations. The depth of this feeling within the military, and presumably within other departments of government, is not yet understood by intelligence community management.

...military warfighters are adamant that they require unclassified materials that can be shared with uncleared coalition forces...

Similarly, there is no place within the government where we come together with industry, academia, and the media to discuss and coordinate similar open source requirements. If Corporate Information Management (CIM) concepts were to be applied to the open source area, we would quickly discover enormous redundancy between government agencies holding the same basic encyclopedic data, and between government agencies and private sector organizations with duplicate or complementary multi-media data. The bottom line: we have not even begun to understand, much less satisfy, our national open source needs.

Existing capabilities are fragmented. Within the Department of Defense (DoD) our most important facility, DTIC, is not part of the intelligence community and was therefore not consulted by the DCI’s Joint Open Source Task Force. Elsewhere, another vital contributor to national intelligence research, the Federal Research Division of the Library of Congress, also was not consulted – and this is the organization which could not find funding for fully 70 percent of the requirements levied upon it by various elements of the intelligence community over the period 1988-1991.

Those elements of the intelligence community which do focus on open source exploitation generally limit their interest to Soviet-related scientific and technical journals, as well as a smattering of multi-lingual print and voice broadcast media. Unfortunately, their databases and products are either reserved for a limited number of analysts, or are such cumbersome compendiums of current news as to be of primary interest to academic libraries desiring to maintain historical records. Notably absent from our community's capabilities are the ability to routinely exploit multi-lingual video broadcasts, "gray literature" (limited edition publications), still photography, and multi-spectral imagery.

The bottom line on this: our classified databases on "Rest of World" (ROW) are empty; our demands are great: only open sources, if exploited in partnership with the private sector, can meet our most urgent needs within the fiscal constraints we must accept as givens. It behooves industry to understand this situation, and to make its own case, extending its assistance, its innovative views, and its open source capabilities and products, into the government.

It becomes obvious, when we realize that we have invested billions of dollars in following the scientific & Technical capabilities as well as the plans and intentions of "the main enemy", that we have at the same time failed to develop the capabilities to follow lesser threats, including those represented by the low-tech brutes (our narco-traffickers who daily present us with "needle in the haystack" detection and tracking difficulties); the low-tech seers (such as the Islamic Fundamentalists whom we still do not comprehend); or the high-tech seers (including both groups such as Japan, and individuals such as the Dutch hacker who penetrated Pentagon computers during Desert Storm/Dessert Shield).

There is no faster, cheaper, more effective way to bring our encyclopedic and research databases in these areas up to speed than to invest in open source capabilities including additional private sector analysts working in active cooperation with government analysts (and not necessarily requiring clearances).
is for this reason that I believe OSINT, and related communications and computer services, are going to be the single fastest growing slice of the CI industry in the 1990s and beyond. OSINT capabilities and products have the obvious additional advantage of being immediately marketable to non-government and foreign customers.

It appears clear that technology is not the showstopper — it is management that is preventing the development of faster, cheaper, and predominantly unclassified intelligence collection, processing, and dissemination capabilities.

Four new capabilities should be established within the executive: a joint government-private sector Center for the Exploitation of Open Sources (CEOS); a National Knowledge Foundation (NKF); an Office of Multi-Special Imagery (OMSI); and a National Open Source Architecture.

A National Open Source Architecture should extend the computer super-highway initiative, integrate the National Research and Education Network, and establish the National Public Network concept advocated by Mitch Kapor. Every citizen should have access to CEOS through such an architecture, and all schools, libraries, research facilities, and corporate reference and analysis centers should be online across the Nation. The Intelligence Communications Architecture (INCA) Project, which has done some fine work in extending the DoD architecture toward the law enforcement community, could conceivably work with other government agencies to give open sources additional prominence within the military, and to extend DoD standards and methods into the civilian community.

The private sector must make a contribution as well. Besides assuming responsibility for global data entry, the private sector must understand and support the need for a new perspective on knowledge and a commensurate adjustment in copyright and patent law. Originators of information should be compensated based on the frequency with which their contributions are accessed, printed, transmitted, extracted from, etcetera. What can no longer be tolerated is the treatment of knowledge as property, and related restrictions on its dissemination.

The private sector can take the lead in establishing national and international open systems and electronic connectivity at an affordable price; the private sector can also take the lead in developing cooperative agreements with foreign enterprises which bring more multi-media and multi-lingual data online.

What this all boils down to is a new concept of national competitiveness, one which moves away from defensive efforts to restrict the transfer of technology and impose trading quotas and other barriers. Instead, national competitiveness is going to depend on national intelligence in a new and broader sense: the ability to quickly recognize change and opportunity, the ability to quickly retool factories and adjust skill mixes, and the ability to "engage our nation" in the business of knowledge.

***************