Open Source Intelligence Clarifies Global Threats

Untapped asset offers partial remedy to budget cuts, multipolar challenges.

By Robert D. Steele

Open source intelligence, which has received mostly short shrift in the past by the intelligence community, offers the potential of illuminating most of the threats that will confront the United States through the balance of the 1990s.

Once known as scholarship, journalism or investigation, open source intelligence (OSCINT) is finally coming into its own. It provides a remedy for those needing analysis of threats for which the existing collection and production capabilities are unsuited.

Open source intelligence also offers a return on investment that far exceeds that of any other discipline. A commitment to OSCINT, 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, it merits serious attention from industry.

As the intelligence community restructures itself and adjusts to changing fiscal and threat environments, three issues are on the minds of those committed to changing the way the community does business.

First, it must be determined what multimedia data sources and products can be collected, processed and sold by the private sector to meet government needs. In other words, the intelligence community, working closely with business, must find a way to define and then privatize much of the government's appetite for open source information.

Next is the requirement to identify the tools, technologies and methodologies already on the shelf or emerging that can be of assistance to government and the private sector as each seeks to exploit open sources for competitive advantage. This approach presents an opportunity to cut costs by standardizing and integrating data bases, applications and technologies.

The intelligence community also must determine what joint endeavors, such as cooperative agreements to digitize and share Third World data, can be assumed by government and the private sector to collect, process and disseminate open source data helpful to the nation's competitiveness.

While a full commitment to this discipline within the national intelligence community has yet to be articulated, a growing number of people believe that OSCINT requires a marked increase in investment. The recent appointment of an open source coordinator by Robert M. Gates, director of Central Intelligence, should provide a focal point for developing a concrete and broad program—in full partnership with the private sector—to meet the unfunded deficiencies in open source multimedia collection, processing and dissemination.

That official will be critical to the nurturing of industrial and academic capabilities and the establishment of a truly national program, which benefits all sectors of government, as well as the private sector.

Outside the intelligence community, under the management of the administrator of the Defense Technical Information Center, an extraordinary semi-official group, the Commerce, Energy, National Medical Laboratories, Defense and Interior consortium (CENDI) brings together managers of scientific and technical information resources and serves as a model for interagency cooperation on open source issues. CENDI, together with the open source coordinator and perhaps with such industrial organizations as the Information Industry Association, offers a basis for coordinating a significant expansion of government investment in open source capabilities and products.

A systematic approach to OSCINT as a separate discipline is the only means by which this discipline can be cultivated and managed in an era of declining funding from Congress. This approach must be unconstrained by clandestine human intelligence management while also fully integrating requirements and capabilities related to public signals and commercially available imagery, including multispectral imagery. Such an effort is best undertaken by a national organization or consortium independent of the intelligence community. This approach also must ensure that government does not act alone, but works closely with all elements of the private sector to form a national partnership.

Defining Open Source

Remembering that intelligence presumes processing and analysis, not simply the dissemination of raw data, OSCINT can be defined as coherent analysis reflecting access to multimedia open sources. Those sources are not classified at their origin, are not subject to proprietary constraints other than copyright, are not produced by sensitive contacts requiring obscuration and are not acquired through clandestine or covert means.

Although existing intelligence community requirements and priorities processes can be considered as applicable to OSCINT, as they are to other disciplines, no real channel exists for consolidating open source requirements and assigning open source capabilities. Despite efforts in the 1980s by the Open Source Council, sponsored by the Human Intelligence Committee, and follow-on efforts by the Information Handling Committee and the Intelligence Producers Council, OSCINT never has received serious support within the intelligence community except as narrowly defined by the Foreign Broadcast Information Service and other community elements that focused on Soviet scientific and technical literature.

Many analysts will testify that their management and their culture are actively biased against the exploitation of open sources. It is much easier for the analyst to seek 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.

Requirements for open sources tend to be ad hoc. No systematic attempt has been undertaken to survey and understand the open source needs of policy consumers, service and department planners, theater commanders and tactical commanders, even with an understanding of community elements interested in open sources. The military, at least, appears to be unanimous in lamenting the classification and handling constraints associated with sensitive compartmented information documents. It also is adamant about requiring unclassified materials that 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.

Forum Needed

Similarly, the government has no place where the intelligence community can come together with industry, academia and the media to discuss and coordinate similar open source requirements. If corporate information management concepts were to be applied to the open source arena, users quickly would discover enormous redundancy among government agencies holding the same basic encyclopedic data, as well as government agencies and private sector organizations with duplicate or complementary multimedia data.

Those elements of the intelligence community that do focus on open source exploitation generally limit their interest to former Soviet-related scientific and technical journals, as well as a smattering of multilingual print and voice broadcast media. Unfortunately, their data bases and products either are reserved for a limited number of analysts or are such cumbersome compendiums of current news that their primary interest is catering to academic libraries desiring to maintain historical records. Notably absent from the community's capabilities is the ability to exploit multilingual video broadcasts, gray literature (unclassified, limited-edition publications), still photography and multispectral information routinely.

Gates recently commissioned a special task force to examine OSCINT issues. The task force report, while limited and tentative in its recommendations, is a promising first step. Given Gates' early guidance explicitly calling for innovative and comprehensive suggestions, and given the growing momentum in both the Executive Branch and Congress for progress in this area, the new open source coordinator can be expected to make substantial inroads across the community and perhaps into the unified and specified commands and the private sector.

Those responsible for supporting the open source coordinator must ensure the inclusion in their deliberations of the private sector and other elements of government outside the traditional confines of the intelligence community. They must take particular care to include the theater J-2s, defense intelligence functional managers and intelligence points of contact for key assistant secretaries of defense—the director of intelligence for special operations and low intensity conflict, for example.

Activities, many of which now are under way, must strive to enumerate existing capabilities. Policy makers also must take care to evaluate the results of earlier studies, as well as the reasons earlier recommendations for change have not been implemented. Any government effort also must address civil libertarian issues; proposed copyright solutions and changes in the law; and the integration of counterintelligence and national competitiveness issues.

OSCINT will play a vital role in meeting many of the U.S. national intelligence requirements in the future. This particularly is vital given the changing nature of war and competition in the 1990s and into the 21st century. Whereas in the past national intelligence has concentrated on the former Soviet nuclear and conventional threat, and open sources have been exploited primarily in relation to Soviet scientific and technical journals, the United States today is facing a kaleidoscope of emerging threats, none of which adequately is addressed by existing data bases, analyst and collection methods.

Besides standard political/military intelligence, an awareness of the urgency of socioeconomic intelligence now exists, and a few analysts are starting to focus on the need for ideo-cultural, techno-demographic and natural-geographic intelligence. National Security Review 29, including for the first time such organizations as the Environmental Protection Agency, is a significant first step in institutionalizing the importance of these new topical areas.

Many military leaders believe that neither technology nor funding is an obstacle to meeting needs for intelligence founded on open sources. The consensus among war fighters, including numerous flag officers at one recent war game, is that community management is the obstacle and that the problems are, by and large, self-imposed.

Lesser Threat Issues

After realizing that billions of dollars have been invested in scrutinizing the scientific and technical capabilities as well as the intentions of what once was the primary foe, it becomes obvious that the intelligence community has failed to develop the capabilities to follow lesser threats, including those represented by the international drug cartels and terrorists, as well as the trauma posed by unscrupulous nations in economic and technology competition.

The only faster, less expensive, more effective way of bringing encyclopedic and research data bases in these areas up to speed is to invest in open source capabilities, including additional private sector analysts working in active cooperation with government analysts. OSCINT and its related communications and computer services are going to be the single fastest growing slice of the command, control, communications and intelligence industry in the 1990s and beyond. OSCINT capabilities and products have the obvious additional advantage of being immediately marketable to non-government and foreign customers.

Solutions suggest themselves. Within the military, war game results, as well as daily contact with consumers approaching one intelligence center, make it clear that unclassified multimedia data and intelligence are priorities. One group went so far as to suggest that the national intelligence architecture for communications and computing should be altered to give primacy to unclassified production and dissemination. Within the military, doctrine must emphasize unclassified data, not only for ease and cost of collection, but also for ease and cost of dissemination with U.S. forces and allies.

Problem Lies With Management

It appears clear that technology is not the show stopper; rather it is management that is preventing the development of faster, less expensive and predominantly unclassified intelligence collection, processing and dissemination capabilities. On the military side, tactical personnel can and should be used to jump-start the process of establishing open source data bases. Given the almost complete lack of 1:50,000 scale military maps for most of the Third World, multispectral imagery is a critical—perhaps the most essential—open source from a military point of view.

To serve the needs of the various departments in and out of the national security community as traditionally defined, a national focal point for open sources is needed across the government. Ideally, it will be independent of all departments and the intelligence community, and it will be able to cooperate fully with the private sector.

The private sector must make a contribution, as well. Besides assuming responsibility for worldwide 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 and so on. The treatment of knowledge as property, and related restrictions on its dissemination, no longer can be tolerated.

The private sector can take the lead in establishing national and international open systems and electronic connectivity at an affordable price. The private sector also can take the lead in developing cooperative agreements with foreign enterprises, bringing more multimedia and multilingual data on-line.

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

• • • — • —

Robert D. Steele, a former Marine Corps infantry and foreign service officer, is a senior civilian in U.S. Marine Corps intelligence. He is a member of the AFCEA Northern Virginia Chapter.

Professional Interchange Offers Best Bet for Intelligence Coups

The acquisition of scientific and technical intelligence by open source is, in many cases, superior to clandestine, human intelligence methodologies. The key is to use properly briefed and cleared U.S. scientists.

Technical and scientific intelligence is gaining increasing attention from the U.S. intelligence community, particularly as economic and trade issues increase in importance.

According to Dr. R. Norris Keeler and Dr. E. Miriam Steiner, the dilemma endemic in established intelligence circles is that case officers generally do not possess the necessary background to pursue scientific intelligence. They add that intelligence officers generally do not have access to the foreign professionals—scientists, technicians and engineers—who possess information unknown in the United States and/or of vital military importance.

"The reputations and expertise of foreign scientists, along with their natural desire to display their own status and accomplishments, strongly militate against a frequent use of deception," explains Keeler, director of technical marketing, Kaman Diversified Technologies Corporation, Arlington, Virginia.

"In a dialog with U.S. colleagues of equal stature, it is difficult for a foreign scientist from a closed or open society to misrepresent the facts."

Keeler, who gained access to a number of highly sensitive research and development facilities in the former Soviet Union, recalls that in 1987 in Kiev he and other U.S. scientists for the first time met face-to-face with the Soviet Union's top nuclear researchers. As a result of this meeting, the United States learned of two previously unknown weapons research facilities, including a highly sensitive computer center in Moscow.

Keeler adds in an interview that the Kiev conference set the stage for a subsequent meeting in 1989 in the West. Much valuable information on nuclear weapons research was gleaned.

Open Source Triumphs

In a recent professional paper, Keeler and Steiner cite another crucial scientific and technical intelligence breakthrough that occurred in 1973 at an international plasma physics meeting in Novosibirsk in the former Soviet Union. At a party, a Soviet scientist revealed advances that were completely unknown in the West.

"These advances," Keeler says, "although later cited in the open Soviet literature, indicated that the Soviets were developing the technology base for a strategic defense initiative program."

Keeler recalls a 1981 plasma conference in Kiev that was attended by several U.S. scientists. It was learned that Soviet scientists were far ahead of their U.S. counterparts in low-density fluid equilibrium and transport properties—areas of research quite important to current weapons systems. The Americans, Keeler adds, also met several then-Soviet scientists heavily involved in weapons research. The upshot is that their work has been intensely studied, and "it is clear that Soviet expertise in the field gives them a unique capability that the United States still does not possess."

A more recent meeting in Leningrad disclosed the existence of a closed institute that boasted first-class scientists. Information aired at this 1986 meeting would have been classified had it been broached in the United States, he says.

Tiny Part of the Effort

Despite these and other scientific and technical (S&T) intelligence windfalls, Keeler points out that "nonclandestine collection by scientists and engineers continues to represent only a tiny part of the U.S. intelligence community S&T efforts. Various intelligence agencies have failed to take advantage of these new opportunities, especially the availability of prominent scientific figures and their latest scientific work, which have increased markedly in recent years as the political climate in Eastern Bloc countries and mainland China has changed."

He charges that the intelligence community currently spends little time and effort on upcoming opportunities, such as international scientific meetings or visits by delegations of scientists. Keeler says that the quality of officers supervising the few existing open human intelligence operations is uneven. He adds that the briefing and debriefing of scientific sources often is conducted by people who are decided strangers to the fields in question.

He points out, however, that the Central Intelligence Agency (CIA) is beginning to see the value of open source intelligence. He notes that former CIA chief William Webster responded most favorably to the paper that he and Steiner co-wrote.

FIRST INTERNATIONAL SYMPOSIUM: NATIONAL SECURITY & NATIONAL COMPETITIVENESS: OPEN SOURCE SOLUTIONS Proceedings, Volume I - Link Page

Previous	OSS '92 Kenneth A. Kovaly, Unique Wire Service Provides Early Intelligence on World's Technical Developments,
Next	OSS '92 Robert David Steele, E3i: Ethics, Ecology, Evolution, and Intelligence...An Alternative Paradigm for National Intelligence (Whole Earth Review, Fall 1992),

Return to Electronic Index Page