The Strategic Use of Open-Source Information

John Gannon

"Open-source information now dominates the universe of the intelligence analyst, a fact that is unlikely to change for the foreseeable future."

John Gannon is a retired CIA officer whose last assignment was Chairman of the National Intelligence Council.

This article is unclassified in its entirety.

The Intelligence Community (IC) is well known as an espionage service. Much less well known is the fact that it is one of the world's biggest information-based businesses, collecting and analyzing open-source information. Open source has long been a high IC priority. Today open-source information has become a major challenge to the IC. The IC response to the challenge is very much a dynamic work-in-progress.

Open-source information is not what it used to be. Ten years ago, "open source" generally meant information from foreign newspapers and the electronic media, which was collected mostly by the Foreign Broadcast Information Service (FBIS). Open source was "frosting on the cake" of intelligence material dominated by signals, imagery, and human-source clandestine collection.

Today, open source has expanded well beyond "frosting" and comprises a large part of the cake itself. It has become indispensable to the production of authoritative analysis. It increasingly contains the best information to answer some of the most important questions posed to the Community. Media reports now are just a small piece of the open-source pie, which comprises a vast array of documents and reports publicly retrievable but often difficult to find in today's high volume, high-speed information flow. Open sources provide vital information for the policymakers, whom the IC serves. Accessing, collecting, and analyzing open-source information, in short, is a multi-faceted challenge that can only be met with a multi-front response or strategy.

This article examines three aspects of the open-source challenge/response dynamic: its critical importance; how the IC is using technology to help the analyst cope with the information glut; and the need for interaction with the private sector.

Critical Importance of Open Source

The world for the IC analyst has changed dramatically since the end of the Cold War. A decade ago *global coverage* largely meant a comprehensive strategy to collect against and analyze the Soviet Union—the IC's single strategic threat. Today, *global coverage* entails the responsibility to assess diverse, complex, and dispersed threats around the world. In additional to traditional intelligence concerns—such as the future of Russia and China, political turmoil in Indonesia, and civil conflicts in Africa—the new environment features many nontraditional missions. The IC now provides intelligence about peacekeeping operations, humanitarian assistance, sanctions monitoring, information warfare, and combating international organized crime, as well as placing greater emphasis on such transnational issues as counterterrorism, counternarcotics, and counterproliferation. Many of these missions are

operationally focused, requiring growing proportions of the analytic and collection work force to function in an *ad hoc* crisis mode.

Open-source information now dominates the universe of the intelligence analyst, a fact that is unlikely to change for the foreseeable future. The revolution in information technology and telecommunications has fundamentally transformed the globe that the IC covers, the services that it provides to consumers, and the workplace in which its people function.

- Information abounds. A growing volume of open-source material is relevant to intelligence needs. Closed societies in the former Soviet Union and Eastern Europe have opened up, and reliable information now is widely available. Fifteen years ago, information on the Balkans was scarce, foreign newspapers took weeks to arrive at an analyst's desk, and policymakers were willing to wait days or even weeks for a paper on the issues.

- Today everything moves faster, and people are better informed. The revolution in information technology has vastly increased the volume and speed of the information flow across the globe and across computer screens. Technology makes analysts more efficient, but it also increases the demand from consumers. Intelligence requirements tend to be sharper and more time sensitive. Analysts often receive newspaper and media reports before the people in the countries where the reports are generated and intelligence consumers will not tolerate waiting days for a response.

- Governments have less and less capacity to control information flows. International organized crime groups, terrorists, narcotraffickers, and weapons proliferators are taking advantage of the new technologies, bypassing governments or seeking to undermine them when governments try to block their illegal activities. Chances are these criminal networks will be using laptop computers, establishing their own websites, and using sophisticated encryption. In the years ahead, these enhanced capabilities will raise the profile of transnational issues that are already putting heavy demands on intelligence collection and analysis.

"Automated analysis tools—data mining and retrieval techniques—provide significant opportunities to help solve the information overload problem."

Dealing with the Information Glut

The enhanced *speed* of communication is a distinct advantage in today's world where intelligence analysts are as comfortable in cyberspace as in the office space of top consumers. The Washington-based analyst can send a message and get a response from a post in a remote country faster than it used to take to exchange notes by pneumatic tube with counterparts in the same building.

The expanding *volume* of open-source information, however, presents a greater challenge. During the Cold War, the job of the IC was to piece together bits of secret information. Each piece of raw intelligence was a carefully acquired golden nugget. Today, the IC is still mining for information but facing an avalanche from both open-source and classified collection systems.

Technology is a major part of the answer to the magnitude of the open-source challenge, but it is no substitute for the other essential component: skilled people. The IC must invest more in technology to provide the analytic tools needed to assess and exploit the vast amount of information available, and it must invest more in people, whose expertise is crucial for prioritizing, interpreting, and analyzing this information. The greater the volume of information to assess, the stronger must be the expertise to evaluate it.

The number of sources and the overall amount of data to which an analyst has access make the process of finding precise information or hidden clues extremely difficult. How can the analyst know where to start looking? What data might be relevant and what should be ignored? When intelligence analysts query databases, they need to know how to ask the questions in a way that will get useful answers, and they need analytic tools to help them extract the right data. Automated analysis tools—data mining

and retrieval techniques—provide significant opportunities to help solve the information overload problem.

Cognitive analytic tools are under development in both the private sector and the government to facilitate management of the information glut, enhancing the IC's ability to filter, search, and prioritize potentially overwhelming volumes of information.

- *Clustering* lets analysts exploit the most useful data sets first, helping the IC perform its warning function. Clustering is particularly helpful when the volume of information, as with open source, makes it difficult to recognize meaningful patterns and relationships.

- *Link analysis* helps to establish relationships between a known problem and unknown actors and detect patterns of activities that warrant particular attention.

- *Time-series analysis* can enable analysts to track actions over time so that unusual patterns of activity can be identified.

- *Visualization* allows analysts to see complex data—including link and time-series analysis—laid out in new and varied formats that promote analytic insight.

- *Automated database population* is designed to free analysts from the tedious and time-consuming function of manually inputting information into databases, reducing the potential for errors and inconsistencies.

"FBIS is developing a single, open-source 'portal'...to be accessible from desktops and expected to be fully operational by 2002."

One of the strongest and most consistent needs of IC analysts is to search and exploit both classified and unclassified information from a single workstation. The Community is working on this and on ways to standardize information and tag it using metadata—or reference information—to make it easier to search, structure, and enter information into databases.

FBIS is developing a single, open-source "portal" that will organize and cross-reference FBIS products, information that FBIS has collected via the Internet as well as other multimedia material.

- The portal, to be accessible from desktops and expected to be fully operational by 2002, will provide analysts with a one-stop shop for all open-source intelligence, whether collected by FBIS or not.

- Material on the portal will be indexed, archived, and accessible via a powerful, easy-to-use search engine.

Enhancing IC Cooperation

Collaborative tools offer a critical opportunity for enhanced cooperation among the IC's 13 agencies, DCI centers, the National Intelligence Council, and literally hundreds of collection and analysis offices. The problem of sharing data among such a large number of organizations is immense, in particular because different agencies have different security standards. Each organization has private intelligence holdings that are extraordinarily sensitive. The IC has to resolve the issue of multilevel security and need-to-know concerns by developing robust and flexible communities of interest using collaborative tools.

New tools are needed to enhance cooperation in two areas:

- Collaboration in the production process to increase speed and accuracy.

- Expertise-based collaboration—to enable a team of analysts to work on a project for several weeks or months.

Several collaborative tools currently available or soon to be deployed include the capability to share both textual and graphic information in real time. These new tools will allow analysts to discuss contentious analytic issues; share information like maps, imagery, and database information; and coordinate draft assessments. This would all be done on line, from their own workspaces, resulting in substantial savings of time and effort over current practices. Future requirements emphasize broad deployment of collaborative tools, relying on mature commercial off-the-shelf platforms performing to standards that allow interoperability across the IC.

Another important aspect of enhanced collaboration is distributed knowledge. The IC will never have a database that contains all information available to all organizations, due to the individual missions of each organization. The ability to share major holdings of multiple agencies and to present an integrated view to the analyst's desktop, however, is critical and possible—but no easy task!

Finally, the IC has some challenges that few private sector organizations face. It deals, for example, extensively in foreign languages—lots of them. FBIS translates and disseminates information in many languages. Automated translation tools are getting better but still do not function adequately. The IC remains heavily dependent on trained linguists.

Working With the Private Sector

The information technology (IT) relationship between the US Government and industry has undergone a dramatic transformation in recent years. By itself, the IC simply cannot stay ahead of the technological curve and it knows it. Today, government no longer dominates research and development (R&D) and the information marketplace—the private sector does. The IT industry's R&D is focused primarily on commercial applications; the IC's requirements increasingly will have to be satisfied by products developed for commercial use. The IC needs to develop close and enduring partnerships in the commercial world to benefit from both the private sector's continuing pursuit of new technology and its best practices in dealing with the open-source challenge.

“The ability to share major holdings of multiple agencies and to present an integrated view to the analyst's desktop is critical and possible—but no easy task!”

In 50 years, the IC has gone from large, stationary mainframes with a handful of dumb workstations to portable multi-service devices that will communicate, compute, and run offices. This represents a dramatic leveling of information costs and affects the way the IC does its work. In many ways, however, the Community still thinks and organizes itself with immobile information systems. It is continuing to invest great amounts in stationary hardware systems, while many of its targets—terrorists, narcotraffickers, and organized crime syndicates—are becoming increasingly mobile in their operations. Perhaps private industry will come up with ways to liberate analysts from their cubicles, while at the same time ensuring the security of their work.

The CIA has developed two organizations to build and sustain outside partnerships: the Office of Advanced Intelligence Tools (AIT) and In-Q-Tel.

- In 1997, CIA's Directorate of Science and Technology and its Directorate of Intelligence collaborated in the formation of AIT. The office works inside CIA with analysts to determine their needs and outside CIA with vendors to identify state-of-the-art cognitive and collaborative tools.

- CIA launched In-Q-Tel in 1999 as a nonprofit corporation designed to bring together the best of the academic, business, and private research worlds to exploit new and emerging information technologies.[1] Its mission is twofold: first, to accept strategic problems and develop a "portfolio" of innovative IT solutions, ranging from exploration to demonstration; and, second, to fuel private research, development, and application of information technologies of strategic national interest for the benefit of all partners.

In-Q-Tel is not designed to conduct research itself; rather, it will orchestrate the work of numerous partner organizations working in teams. In-Q-Tel's initial projects focus on four interrelated intelligence challenges:

- *Agency use of the Internet*, particularly Internet search and privacy issues.

- *Information security*, a crosscutting issue that permeates all organizational functions. In-Q-Tel will engage information security from the perspectives of hardening and intrusion detection; monitoring and profiling of

[1] The new corporation was first launched in February 1999 as In-Q-It, but changed its name to In-Q-Tel in December 1999 to prevent confusion with the financial software giant Intuit. "In-Tel" is self-explanatory, while the "Q" stands for technical innovation—derived from the James Bond character who developed Bond's spy gear.

information use and misuse; and network and data protection.

- *Analytic data processing capabilities*, including geospatial and multimedia data fusion/integration, all source analysis, and computer data forensics.

- *Distributed information technology infrastructure*, to facilitate data dispersal to multiple organizations/agencies anywhere in the world.

The IC leadership recognizes that partnerships with outside technical and academic experts, as well as vendors, are essential to enabling us to stay on top of the information technology curve. Among analysts, the attitude and behavior toward the outside world is slowly changing, but the IC needs to provide more incentives for analysts to get out from behind their desks to engage with substantive experts and other outside sources of useful—and increasingly critical—information that cannot be captured by clandestine collectors or traditional open-source collectors such as FBIS. This is an imperative, not an option. It has been said that, "Opportunities are like sunrises. If you wait too long, you miss them." The IC cannot afford to miss today's opportunities because it is too inwardly focused. It does not intend to do so.

"By itself, the Intelligence Community simply cannot stay ahead of the technological curve and it knows it."

Conclusion

For most of its history, the Intelligence Community has operated as an industrial enterprise, with compartmentation as a key operating metaphor. In the process, a set of impressive organizations has been created; however, they are now being overtaken by events. In the post-industrial world pervaded by information technology, networks defeat hierarchies, and agility becomes a prerequisite for organizational success. Even with the impressive gains of the past few years, dealing with the open-source challenge will necessarily be a work-in-progress for some time to come. Open source is not a traditional collection challenge, and there is no single solution. Meeting the challenge requires a multi-front strategy, and it will take time for the IC to get this right.

The IC recognizes that it can succeed only if it exploits the changes taking place in the information revolution and in information industries. The Community always will have security concerns but cannot allow them to deter it from taking advantage of the opportunities inherent in the emerging environment.

The leadership has committed the IC to a corporate strategy that will leverage the best practices and resources of the whole government and the private sector to provide the President and US policymakers the information advantage they need.

Approved for Release: 2014/09/10 C06122487