



**NATO
OPEN SOURCE
INTELLIGENCE
READER**



FEBRUARY 2002

OPEN SOURCE INTELLIGENCE READER

TABLE OF CONTENTS

INTRODUCTION

- Introduction to the NATO OSINT Reader2
- Open Source Intelligence: The Challenge for NATO3

THEORY AND HISTORY OF OSINT

- Understanding Open Sources9
- The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies..... 12
- Review Essay - Open Source Intelligence.....17
- Grey Literature.....24

APPLICATION OF OSINT

- Open Source Information30
- New Risks of Crisis - Fresh Perspectives From Open Source.....35
- Secrets For Sale: How Commercial Satellite Imagery Will Change the World.....39

INTERNATIONAL VIEWS OF OSINT

- Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Within the Intelligence Community56
- Open Source Intelligence: What is it? Why is it Important to the Military?64
- The Privatisation of Intelligence: A Way Forward for European Intelligence Cooperation - "Towards a European Intelligence Policy"74
- Open Source - Lessons Learned80
- Optimising Open Source Information Sharing in Australia: Report and Policy Prescription – (Part IV, V).....86
- Open Source Intelligence a ‘Force Multiplier’95

REFERENCES

- Collection and Use of Open-Source Intelligence98
- Directory of Resources104

INTRODUCTION

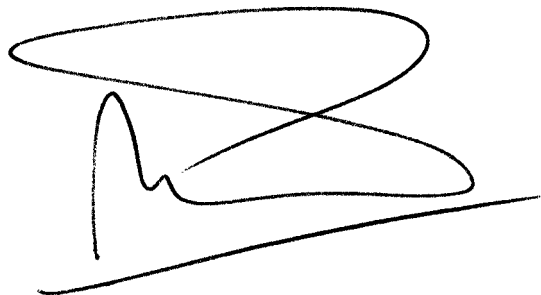
INTRODUCTION TO THE NATO OSINT READER

This publication supplements the *NATO Open Source Intelligence Handbook*, published in November 2001, which provided preliminary information on the subject of Open Source Intelligence (OSINT). The *NATO OSINT Reader*, a focused collection of articles and reference materials by worldwide experts, is designed to give commanders and their staffs the theoretical, historical, practical, and international background necessary to understand how this discipline has evolved. The increasingly robust array of open sources available enables commanders to attempt to satisfy some of their information requirements themselves rather than resorting to directing Requests for Information (RFIs) elsewhere.

The *NATO OSINT Reader* provides comprehensive information and various perspectives on OSINT, including:

- Expositions as to what OSINT is and why it is so important to the military forces of today and tomorrow;
- The theoretical framework of collecting, analyzing, and reporting OSINT information;
- The history of OSINT, particularly as practiced by the NATO nations;
- The application of OSINT to real-world situations both current and future as well as historical;
- International views of OSINT, including but not limited to the views of NATO members; and
- References for further reading and study.

The NATO OSINT Reader has been prepared by the staff of the Supreme Allied Commander, Atlantic, Intelligence Branch in collaboration with staff from the Supreme Allied Command, Europe (SACEUR), and the original sponsor for most of these articles, Open Source Solutions Inc. The *Reader* and the *Handbook* will be supplemented by a third companion document, *Intelligence Exploitation of the Internet*. The information in this trilogy is relevant to all NATO commands, task forces, member nations, civil-military committees and working groups, and such other organizations that may be planning or engaged in combined joint operations.



F. M. P. 't HART
Rear Admiral, Netherlands Navy
Assistant Chief of Staff, Strategy

OPEN SOURCE INTELLIGENCE: **THE CHALLENGE FOR NATO**

Commodore Patrick Tyrrell OBE MA LL.B Royal Navy
Commander, Defence Intelligence and Security School, UK
<mailto:patricktyrrellrn@cs.com>

The dramatic changes in the strategic environment have had profound effects on the way in which NATO conducts its business. Indeed, the changes have altered the very nature of the business in which the Alliance is involved. The most obvious of these is the incorporation of the first three new members of the Alliance for 16 years and the development of the Partnership for Peace initiative. The shift away from the military focus of the Alliance in the days of the Cold War towards a more politically astute and centred organisation was started by Secretary Baker in 1989 when he called upon the Alliance to look towards helping set the new agendas for Europe in the 1990s. At the same time, there have been a proliferation of requirements for intelligence support that are inherently non-traditional; including the readjustment of borders, the study of new migrations, concerns over environmental threats and the need to collect and analyses at the social and economic levels.

Change is never an easy bedfellow and sixteen sovereign nations often have widely differing national interests. The Palmerstonian Doctrine still holds sway in today's strategic environment¹ and the concept of "*realpolitik*" will mean that such national interests will continue to dictate how nations conduct themselves both in private and on the world stage. International organisations like NATO and the UN have provided a forum for nations to be able to develop common approaches to common problems but I still see the attitude of one British Trades Union leader who, during a dispute, was heard to remark: "*I shall negotiate, but never compromise*". Despite this requirement to achieve consensus and the painfully slow process at times, NATO has made major strides in restructuring and reorganising itself in preparation for the welcoming of new members. There is, however, a clear need to develop a common view of the joint or coalition operating environment if co-operative efforts are to succeed.

One of the most sensitive areas of any military alliance is that of the collection, analysis and dissemination of intelligence. NATO's intelligence structure relies primarily upon intelligence inputs from member nations with only a limited capability, especially in peacetime, for the generation of its own raw data. As such, the NATO intelligence baseline and its standard operating procedures are all centred on a highly classified basis and often exclude unclassified, open sources of intelligence, including commercial imagery.

The concept of an "*information revolution*" has been well developed over the past decade. It is a result of this revolution is that it has allowed us to gain access to unparalleled quantities of data and to retrieve, manipulate, sort, filter, interrogate, digest, plagiarise, and generally bend it to our bidding. Reality is somewhat removed from this in that much of the available

¹ Palmerstone's speech to the House of Commons, 1 March 1848: "*We have no eternal allies, and we have no perpetual enemies. Our interests are eternal, and those interests it is our duty to follow*"

information remains in a format that is not susceptible to digital manipulation, and the search engines are often only as good as the operators who manage them. However, modern technology clearly gives us a tremendously powerful tool with which to conduct information analysis. The revolution has been spurred by the simultaneous collapse of the bi-polar world and the freeing of much data, formerly held as classified. Within this vast “*cyberstore*” of information there will be much that is inaccurate, irrelevant or, simply, out-of-date. It was the veteran US journalist, John Lawton, who in 1995 said: “*It is the irony of the Information Age, that it has given new respectability to uninformed opinion*”. It is very tempting to believe that all that scrolls before you on your screen is a quality product!

The revolution, so far, is, essentially, a technical revolution with the development of cheap yet fast computer systems capable of achieving the storage capacities and speeds necessary to search through vast quantities of data. There is, however, a necessary corollary, and that is the development of the human skills necessary to the effective use of the information tools. This is more than the ability to “*surf the net*” and to access on-line databases. It requires an understanding of the subject matter, the techniques relating to computer searches, the ability to make use of an increasing array of sophisticated data-mining techniques, an understanding of where information is likely to be and how to obtain it even if it is not digitally stored in an appropriate database. Perhaps most importantly, the revolution requires dramatic changes in culture, security, and procurement precepts such that the role of the intelligence analyst changes. As the former Deputy Director of Central Intelligence Agency noted at a recent international conference on open source intelligence, the analyst must now “*know who knows*” and be able to identify, task and interact with subject matter experts outside the intelligence community, most of whom do not hold traditional clearances.

Intelligence Skills:

The traditional view of intelligence communities is that they are already aware of the uses (and abuses) of open source material. What has changed, however, is the quantity and quality of available, unclassified material. Many of the skills required of the *information mining engineer* are those already inculcated in the intelligence analyst. The ability to comprehend the overall problem, whether at the tactical or strategic level, is an essential prerequisite for designing an appropriate search policy. The analytical skills allow him to filter the irrelevant, identify the valid and discard the inaccurate. It is important that analysis skills are not considered to be synonymous with searcher or librarian skills, however; the *information miner* must be able to understand where the unclassified information fits into the broad picture. This will demand access to all source data, including where necessary to classified sources. It is this breadth of vision which must be developed if the analyst is not to be myopic in outlook.

Sources of intelligence:

Traditionally, intelligence services have concentrated on classified sources for their analysis. It is true that they have always relied on identifying unclassified sources to provide verisimilitude to the classified product, but the emphasis has remained on the provision of a classified report, issued to those suitably cleared to receive it. In the past, information has been classified either to protect its source or its subject matter. As we approach the millennium, traditional intelligence principles are being turned upside down. As noted by Hugh Smith and cited by Sir David Ramsbotham, “*Intelligence (for coalition and UN operations) will have to be based on information that is collected by overt means, that is, by*

methods that do not threaten the target state or group and do not compromise the integrity or impartiality of the UN (or NATO)”.

The development of modern information systems has also made much of the material, formerly only available from classified sources, readily accessible to any who wish to seek for it. Overhead imagery, for example, is now being supplied from commercial sources for a number of non-military tasks including land use, planning, exploration, etc. The resolution of these systems is already good enough for a number of military applications.

Open Source information:

As we have seen, not all the available open source information is conveniently available on interconnected computer systems. Much remains in archives, libraries and other repositories; some is available only on request from government sources and some is in private collections. Availability of information, or at least the ability to access it, is not always international and can only be obtained by someone located in the vicinity of the data. According to US studies, some 80% of what a commander requires, is neither digital in format, in English or, often, unpublished. It will be up to the subject matter expert to bring these inchoate sources into a coherent product.

Open source data is increasingly important to support the intelligence function. The increasing ability to successfully mine data from a large, incoherent series of sources, allows analysts to build up detailed composite pictures of their area of interest. Open source analysis is not a substitute for the traditional classified work, the analyst can use the open source view to be able to ascertain what additional information might be required on a particular subject and, having identified the gaps in his knowledge, task the increasingly scarce resources to target those gaps with whatever tools may be appropriate. Essentially, open sources provide for the foundation for classified collection management, while also providing the context and, importantly from the intelligence perspective, sometimes providing cover for classified sources and methods and often giving evidence as to where new classified studies might be best targeted.

NATO/PfP Requirements:

NATO and the Partners for Peace need to be able to build up a degree of mutual trust and compatibility if the PfP process is to succeed, particularly in the case of Russia. There are few areas as sensitive as the intelligence arena and co-operation in such areas would provide a strong confidence building measure and enhance stability. The new high-level councils, including the recently formed Permanent Joint Council (PJC), will require supporting by a suitable formed intelligence group. Although, as in the past, national intelligence capability can provide an input to individual delegations, the Alliance itself will require independent advice. This can be provided by the existing NATO intelligence staff but would be considerably enhanced if there were to be a NATO/PfP open source facility, working jointly with the existing NATO staffs.

Open Source Programme:

Within the NATO/PfP Open Source Programme, there would be a separate and distinct NATO/PfP Open Source Bureau of modest proportions, specifically tasked with the

acquisition and analysis of information in support of the NATO/PfP secretariats, made up of personnel seconded from all participating nations. There are three potential options:

- establish a “virtual” bureau based on national intelligence staffs operating from their respective national capitals. This is a “Federated Bureau”.
- establish a single NATO/PfP bureau at one location fully staffed by a representative group of all member nations. This is a “Central Bureau”.
- Composite bureau of nationally based staff with a co-ordination group centrally located. This is a “NATO Web”.

The role of the programme, however formed, would be to provide, both on demand and as a routine service, high quality and reliable access to unclassified material. Within the current NATO nations, unclassified material has always been relatively easy to procure. A distinct advantage to NATO will be to have access to those databases and archive which, hitherto, have not been readily available from the PfP nations. The programme would make effective use of existing commercial service providers as well as those of individual member nations. Although the programme will demand highly trained personnel, there is no necessity for the programme to come under the direct control of the intelligence staffs. The intelligence staffs will, undoubtedly, be customers for the product but they will only be one of several potential customers. The bureau will be equipped to handle a wide range of queries, many of which will be easily answered with reference to on-line sources for NATO and PfP staff officers, military headquarters and component commands. Access would be via telephone, fax, and e-mail with clear performance targets to be met. The depth of expertise required will increase depending upon the level of service being provided:

- Periodic awareness service - single page digests on demand
- Search and retrieval - including use of commercial databases
- Primary in-depth research with the identification of appropriate subject matter expertise to meet the customer’s requirement
- Strategic forecasting, including that for scientific and technical trends.

The importance of commercial imagery as a foundation for a common operational appreciation cannot be understated. For a relatively modest outlay, commercial imagery could be acquired which would have considerable utility both within NATO and in member nations. The imagery currently available can readily create the 1:50 combat charts which do not exist for much of the region today, as well as providing for the provision of precision munitions targeting information and for three-dimensional, interactive, flight mission rehearsals.

The function of the programme would be to provide what one commentator has described as “*just enough, just in time*” intelligence, clearly focused upon the customer’s requirements. It would be designed from the outset to add value to information available to Alliance and national decision makers. In some cases, where the query is complex or the customer is a high priority one, there may be a requirement to provide what would, in commercial terms be an account manager whose task would be to act as an interlocutor between the customer and the programme information staffs. His role would be to assist the customer in focusing his requirements and in the management of the subsequent search and retrieval.

Implementation:

The cost of implementing such a programme is considered to be modest. Much of the required interconnectivity is already in place between the respective capitals and the NATO HQ. The three options would provide for a range of staff costs depending upon whether the programme was set up as a single site entity or as an interconnected, federated system of cells. The advantage of the former is that the members of the programme are clearly linked as a team but the federated solution may allow for better insinuation of the individual open source programme cells with their respective parenting organisation within each nation. This could be augmented by the provision of a co-ordination staff at a convenient site and the use of exchange personnel between the national cells.

There would be a requirement to train the programme staff to a common standard to ensure that all participating nations could contribute fully to the activities of the organisation. Training needs analysis would need to be done to support not only the initial training requirements but also the longer-term needs of the programme. The DISS at Chicksands in the UK is one of several places where such training could be given.

The provision of such a bureau need not necessarily be a NATO/PfP owned facility: out sourcing of the organisation would save start-up costs and transfer risk to the private sector. The programme would then charge NATO and PfP nations for their services with clear performance criteria laid down for the delivery of the product. This would have the additional advantage of further distancing national intelligence staffs from the provision of the service and, inter alia, allow them to concentrate on their primary functions. It would be important that any selected company would be required to select staff from all participating nations, especially those of the PfP, to ensure the continued national commitment to the overall programme. As an interim alternative, a small contract could be let for the provision of specific open source intelligence products to the NATO/PfP programme. The core value of this programme, however, is the creation of a shared NATO/PfP open source intelligence architecture with interoperable hardware and software. To achieve this ultimate goal, however, will require this programme to be fully integrated into the C4 planning and resource management aspects of NATO and be fully supported by all members of the Alliance.

The key posts in this organisation would be at the senior management level; the director of the programme would have to be chosen for his vision, intellect and management capabilities rather than for the “cut of his cloth”. It would be essential that these key personnel had the full support of the NATO/PfP Board. Initially, no more than six full time civilian members are envisioned, with additional staff provided from member nations’ military and civilian personnel. Such an Open Source Programme will give a positive, relevant and productive core capability, able to be developed further as the participating nations become more used to sharing information. It will have important implications for future coalition operations whether composed of NATO/PfP or of a wider range of nations. It represents a single, positive step to engender trust, cooperation and confidence between Alliance and PfP members and also gives important skills to their intelligence staffs as we approach the *information millennium*.

Conclusions:

- Open Source programme for NATO is viable option for NATO/PfP

- Open Source programme would provide a significant confidence building measure for PfP nations
- An open source programme will allow PfP and candidate nations to participate at an early stage in the intelligence process within the Alliance
- An open source facility is complementary to existing intelligence functions and will allow the traditional NATO intelligence community to concentrate on other core skills
- The ability to acquire and exploit commercial imagery and external subject matter expertise will assist in the development of a clearer understanding of the joint NATO/PfP operational environment
- Open source analysis uses traditional intelligence analytical skills, although some additional talents are required to ensure effective and rapid retrieval of data
- There would need to be an assessment of the validity of the product
- Training of personnel for such a programme can be easily developed and conducted at a number of places of excellence throughout the Alliance
- The programme would provide 24 hour access to NATO and national staffs with specific “customer” targets established in relation to the delivery of the required analysis
- The entire operation could be undertaken by a commercial provider but the involvement of staff from all member nations would be an important consideration

THEORY AND HISTORY OF OSINT

UNDERSTANDING OPEN SOURCES

**Eliot A. Jardines, Open Source Publishing Inc., <http://www.osint.org/>
Excerpt from “Open Source Exploitation: A Guide For Intelligence Analysts”,
produced by Open Source Publishing Inc. for the Joint Military
Intelligence Training Center (JMITC)**

Open Sources Defined

The Intelligence Community has an official definition for open source information. It is contained in a Director of Central Intelligence Directive (DCID) which established the Community Open Source Program Office, effective 1 March 1994. The definition is:

Open source information for purposes of this directive is publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation), as well as other unclassified information that has limited public distribution or access. Open source information also includes any information that may be used in an unclassified context without compromising national security or intelligence sources and methods. If the information is not publicly available, certain legal requirements relating to collection, retention, and dissemination may apply.(1)

An important subset of open source information is called Grey Literature. The Interagency Grey Literature Working Group (IGLWG) is defined as follows:

Grey literature, regardless of media, can include, but is not limited to, research reports, technical reports, economic reports, trip reports, working papers, discussion papers, unofficial government documents, proceedings, preprints, research reports, studies, dissertations and theses; trade literature, market surveys, and newsletters. This material cuts across scientific, political, socio-economic, and military disciplines.(2)

Organizations that typically generate the largest quantities of grey literature include: research establishments (laboratories and institutes); national governments; private publishers (pressure groups/political parties); corporations; trade associations/unions; think tanks; and academia. Open source information, then, is acquired from newspapers, television and radio broadcasts, books, reports, journals, and photographs and other images. Of course, these sources have been used successfully in the intelligence production process for many years. What is different now is that there has been an explosion in the quantity and variety of open source material published electronically and readily searchable on-line. The ability to search the World Wide Web or in essence, millions of pages of text within seconds, has proven to be the major impetus for the rise in popularity of open source information as a viable and fruitful component of the all-source process.

Open Sources Quantified

In 1992, during his tenure as Deputy Directory of Central Intelligence, Admiral William O. Studeman reported on the contributions and capabilities of open sources. In an article for the American Intelligence Journal, Admiral Studeman wrote:

We have identified some 8,000 commercial databases - and the vast majority has potential intelligence value. The number of worldwide periodicals has grown from 70,000 in 1972 to 116,000 last year. The explosion of open source information is most apparent in the Commonwealth of Independent States (ed. The former Soviet Union), where today, there are some 1,700 newspapers that were not published three years ago. FBIS (Foreign Broadcasting Information Service) monitors over 3,500 publications in 55 foreign languages. And each day it collects a half a million words from its field offices around the world and another half a million words from independent contractors in the U.S. - that's equivalent to processing several copies of War and Peace every day.(3)

Open source information is available from a wide variety of sources and presented in a variety of formats. Surprisingly, most of the world's information (some estimates are as high as 80%) remains in printed form stored in libraries or other repositories. Despite the very rapid growth in the quantity and variety of information in electronic formats, the ratio between traditional hardcopy and electronic format information may not be changing significantly because the volume of printed material has also increased in the information age.

Recently, the total quantity of data available on the Internet was estimated to be six terabytes (one terabyte = 1,000 gigabytes).(4) While that may seem to be a tremendous amount of data, a community library containing 300,000 volumes has about 4 terabytes of data. The largest library in the world, the United States Library of Congress has more than 100 million publications. So, while data on the Internet can be searched quickly, the total data available represents only a small percentage of the available open source information. However, the growth of data on the Internet is explosive. A large US telecommunications company has estimated Internet traffic growth at a rate of 30% per month! At that rate, Internet traffic volumes doubles roughly every ten weeks.

It is also important to understand the volatility of Internet data. In a 1997 article, Internet guru Brewster Kahle indicated that the average life of an Internet document was 75 days.(5) Whole Internet sites appear and disappear frequently and without notice. For the open source analyst, this means that any attempts to catalog Internet sites will be difficult and require continuous maintenance to stay current. In short, it may not be enough to simply bookmark Web resources in a browser, effective open source exploitation may require actual archiving of Internet sites.

Contribution Of Open Sources To The All-Source Product

Various attempts have been made to measure the contribution of open sources in the production of finished intelligence. Depending on the topics and the speaker, estimates range from negligible to 80%. Even the most enthusiastic supporters of open sources admit that they are just one of the several sources which support the production of finished intelligence products. One of the most widely quoted descriptions of the role of open sources states:

Open source intelligence provides the outer pieces of the jigsaw puzzle, without which one can neither begin nor complete the puzzle. But they are not sufficient of themselves. The precious inner pieces of the puzzle, often the most difficult and most expensive to obtain, come from the traditional intelligence disciplines. Open source intelligence is the critical foundation for the all-source intelligence product, but it cannot ever replace the totality of the all-source effort.(6)

Notes:

1. Director of Central Intelligence Directive (DCID) 2/12 effective 1 March 1994. This directive established the Community Open Source Program Office (COSPO) that was charged with development, coordination and oversight of open source efforts throughout the US Intelligence Community. COSPO has recently been reorganized and renamed the Community Open Source Program (COSP) an organization within the Foreign Broadcast Information Service (FBIS).
2. Definition provided by Mr. Bruce Fiene, Executive Secretary, STIC Open Source Subcommittee in a memo dated 15 October 1994.
3. Admiral William O. Studeman, "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community" American Intelligence Journal, Spring/Summer 1993, pp. 11-13.
4. Steve Lawrence and C. Lee Giles, "Accessibility of Information on the Web," Nature, July 8, 1999, 107. The authors, both NECI researchers, indicated that as of February 1999, the publicly indexable World Wide Web contained 800 million pages, comprising six trillion bytes of text and three trillion bytes of images.
5. Brewster Kahle, "Preserving the Internet," Scientific American, March 1997, 82.
6. Dr. Joseph Nye, then Chairman, National Intelligence Council, speaking to members of the Security Affairs Support Association at Fort George G. Meade, Maryland, on 24 April 1993.

THE ROLE OF OPEN SOURCES AS THE FOUNDATION FOR SUCCESSFUL ALL-SOURCE COLLECTION STRATEGIES

**Mr. Charles Allen, Assistant Director of Central Intelligence
for Collection, keynote speaker on Requirements, Collection,
and Current Awareness: The Human Dimension**

Thank you, Robert, for your kind introduction. I am pleased to be able to address a topic of such importance to the Intelligence Community. The conference program (and Robert's kind introduction) bills me as a "KEYNOTE" speaker. In fact, we all know that, because of the World Wide Web, I am also a "KEY WORD" speaker. My talk will be posted on the Web, subject to key-word retrieval—electronic "pull". Many keywords, by happenstance, will cause this paper to be delivered to the desktops of people who are looking for something entirely different. It serves, however, to point out a problem that the Intelligence Community faces—which all of us face. There is such a volume of open source information that we must rely on information technology to help sort it out, and that technology is quite crude.

For the intelligence analyst, the very richness of open source, and the imprecision of retrieval, pose barriers to effective use of open sources. Compare this to the processes in place for dealing with one of the other intelligence disciplines ... or, "INT's." Each of the other INTs has costly and elaborate organic processes that sort out the "signal" from the "noise"—separating the accurate agent report from gossip and invention, separating the real airplane from the plywood decoy.

Take the HUMINT machinery, for example: Analysts and policy makers anticipate their need for information and make those needs known to the HUMINT community—that fabled apparatus of spies and case officers—and by extension to military attaches and to foreign service officers. Overtly and covertly, US Government personnel seek out individuals who possess or have access to the information that will improve US policy making and warn us of hostile intent. The sources, themselves, are often in a good position to sort out wheat from chaff, and the information made available to us by these sources is further refined in the process of drafting reports sent back to Washington. Here in Washington, additional scrutiny is applied before a report is released to the analysts. Disingenuous reports are suspected, vetted, and usually discounted. Repeated interactions with the field, often all the way back to the source, often take place. The bottom line is that knowledgeable humans apply their insights at every stage in the HUMINT process, from initial tasking through the satisfaction of that tasking.

The SIGINT System, too, invests in a costly processing apparatus of human experts to refine requirements and sort out and add value to intercepted information. This quality-assurance overhead is above and beyond the technical machinery needed to make electronic blivots sensible to people. Target by intelligence target, SIGINT analysts laboriously refine mountains of ore to find nuggets of information. A sizeable fraction of the SIGINT System is devoted to winnowing down the raw data so that only the more meaningful information flows to the all-source analysts and policy makers.

Likewise, the Imagery system has elaborate, human-intensive tasking and analytic processes. Imagery-savvy people help the all-source analysts better define their questions and translate them into imagery tasking. And, it is still humans, today, who transform the uncountable, esoteric pixels into meaningful, digestible, pieces of hard information. Still others augment the reports with, annotated, easily understandable pictures ("happy snaps"), which illustrate the points.

But, what about the US Government's open source enterprise? What similar investments do we make? What similar processes do we operate? A knowledgeable audience, you know the answers. Indeed, you probably anticipated the questions. Only for traditional foreign media—newspapers, radio and TV—is there a semblance of a US Government “system” in place. The Foreign Broadcast Information Service, FBIS, is miniscule in comparison to the machinery of the other intelligence collection disciplines. Yet, it provides a service of common concern for the U.S. Government by seeking out, translating, and reporting foreign media information. Proud of its tradition, which prophetically antedated Pearl Harbor, the Foreign Broadcast Information Service advertises its "smart front end"—dedicated human beings with cultural ties to the countries of interest and continuity with the issues. This smart front end has made FBIS a premiere reporter of international events.

However, the distribution media for open sources are changing, the bandwidth increasing and the cost decreasing. By lowering the effective entry cost of publication, new open sources spring up daily and the overall volume is increasing dramatically. It is not clear that the strategy of a human-powered "smart front end" will see us into the future ... not clear that it "scales up." To its credit, FBIS is engaging the new technology on its own terms. Whether we are keeping pace or simply falling behind less quickly is an open question. Investment resources for new technology are scarce and the technology cannot yet deliver the precision of selection which we attribute to the experienced human operators.

Having hewn to your conference theme of "the human dimension," and having described what is, I should like to try out on you my ideas about what should be. Then, time permitting, I will close on the advertised topic of "*The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies.*"

The history of how I came to be the Assistant Director of Central Intelligence for Collection is one of spirited negotiation ... not so much about Charlie Allen the person ...(although modesty permits me to admit there was some of that.) More to the point, there was spirited negotiation about the roles and mission of the ADCI/C, ... about the value such a position could add, ... indeed, about the very need for such a position.

Many who vied to architect the "New, Improved, Post-Cold-War" Intelligence Community believed we should institutionally reorganize around the "core business processes" of intelligence:

- Collection with attendant Processing; and,
- Analysis and Production.

Or, if wholesale institutional reorganization were more than the system could bear, then, clamored the reinventionists, there should be positions created to embody the management of these core businesses. In the event, Congress created two such positions: the Assistant Director of Central Intelligence for Analysis and Production; and, the Assistant Director of

Central Intelligence for Collection. Not surprisingly, Congress as creator decided these should be confirmatory positions; the Administration was less sure.

Mr. John Gannon serves as ADCI/AP and I serve as ADCI/C. Neither of us has stood for confirmation, but our nominations were made with the advice and consent of the Congress. This is largely a distinction without a difference. Both of us enjoy the strong support of Director Tenet and of the Congress. (About the only difference I can make out, is that you should not refer to me as "The Honorable Charles E. Allen".)

The logic of the proposed reorganization, and ultimately the logic of my position was and is that the collection disciplines—SIGINT, HUMINT, IMAGERY, and to a lesser extent MASINT and Open Source—were perceived as being inward looking. Referred to as "stovepipes", the "INT's" were thought to be collectively less efficient even as they strove to be individually more efficient. The whole was no greater (and perhaps less) than the sum of its parts.

The theorists would say that we were "optimizing locally" as opposed to "optimizing globally" and the changed state of the world to which intelligence speaks is less tolerant of local optimization. Said simply, we can no longer afford the luxury of collection stovepipes given these changes. Principal among the changes, are four that I should like to mention briefly:

- First is the thankful loss of the principal adversary, the Soviet Union, which had the means, and perhaps the motive to devastate the United States.
- Second, and less thankfully, the principal adversary has been replaced with a diversity of asymmetric adversaries, who would challenge us with biological, chemical, and perhaps cyber weaponry.
- Third is the decline in resources allocated to intelligence.
- Fourth is the loss of our collection monopoly in reconnaissance imagery ...which, since it is an open source issue, deserves a digression here.

The coming commercial availability of high quality space imagery—coupled with resource constraints on the next generation of U.S. Government imagery satellites—means a potential adversary could access imagery functionally equivalent to that of US forces. For those of us in the U-2 generation, accustomed to an ever more commanding lead in imagery products, this is a watershed event. We may be looking at the culmination of Eisenhower's "open skies" policy ... which takes some getting used to. More frightening, we may have reached the point where even dramatic improvements in US Government-unique imagery assets could not alter the equation. Even though we might know everything, the adversary might still know too much. Imagine trying General Swartzkopf's "Hail Mary" left hook in the desert against an imagery-informed adversary.

The *Eminence Grise* of Open Source, our host Robert Steele, is quoted as strongly recommending "... that all managers and analysts take the time to understand what commercial imagery and geospatial data can contribute to their production process. Very high resolution commercial imagery, with processing, is available for only \$10.00 to \$40.00 a square kilometer. No intelligence product should be regarded as complete until it has considered the possible value-add of commercial imagery."

The US Government may wring its hands about the likelihood that potential adversaries might make better and better use of better and better open sources. However, I suspect many in the audience worry that the US Government, itself, will fail to take advantage of commercial open source offerings. In some ways the Intelligence Community's flirtation with commercial open sources mirrors the broader embrace of commercial, off-the-shelf products by the Department of Defense—an embrace likened to that of two porcupines, who do it very, very carefully.

As a shopper, the US Government is a prisoner of its procurement legacy—a history of monopolizing the market, perceiving its needs to be unique, and reimbursing vendors for costs incurred. This manifests itself in our nit-picking the content of commercial offerings, and our persistent, prurient interest in production cost, rather than market price. If we are to make better use of commercial, off-the-shelf, offerings our motto should be: **adopt, adapt, and stimulate.**

Our first recourse should be to simply adopt from the available offerings those which closely approximate our needs. Or, we should adapt our processes, where possible, to make use of available offerings. Failing that, we should advertise our needs and stimulate vendors to fulfill those needs within their commercial practice.

Some have suggested that each of the Community's components have a "gold team" whose job it would be to advocate, unabashedly, the use of commercial offerings. Another suggestion is aggressive use of "Activity-Based Costing" (ABC), which would show how much each in-house process really costs. This works in tandem with another suggestion, that we take better advantage of Federal Acquisition Regulations (FAR's) which already permit market-price procurement without demanding proprietary cost data.

The glue that holds these suggestions together is an independent estimate of the true worth of a product. We should adopt commercial offerings gleefully if their market price is less than their intrinsic worth to us, and less than the cost of doing it ourselves. (That is why I am committed to develop better measures of effectiveness for all US intelligence collection activities.)

Now, having digressed to establish my *bona fides* as a friend of open source and a champion of commerce, let me return to the job of the ADCI/C and the ostensible topic of my talk: "*The Role of Open Sources as the Foundation for Successful All-Source Collection Strategies.*" Permit me to describe my *Strategic Intent for Intelligence Collection*. The lineage of my vision traces back, directly, to the Director's *Strategic Intent*, which, in turn, flows from the President's *National Security Strategy for a New Century*. Countering the threats to U.S. interests—regional or state-centered threats; transnational threats; spread of dangerous technologies; foreign intelligence inroads in the US; and failed states—the President's *Strategy* stresses, foremost, the need for integrated approaches. In similar vein, Director Tenet's first objective is to "unify the Community through Collaborative Processes."

For my part, the outcomes to which I propose to commit the collection community are to:

- Institutionalize and make routine collaborative cross-INT activities so as to optimize collection resources across disciplines and controlling authorities.
- Enable consumers to express their needs easily and to track the satisfaction of those needs through collection, processing, exploitation, and dissemination.

- Structure an integrated collection system that is sufficiently agile to respond to dynamic needs.
- Maintain balance in attending to short-term and long-term needs and ensure the development of collective capabilities that address long-term needs.
- Rationalize collection resources with bottlenecks in processing, exploitation and dissemination.

As you can see, these preferred outcomes all share the flavor of collaborating, integrating, and optimizing across what have traditionally been collection stovepipes. Open source has always been the backdrop against which the individual INT's play. The first step in formulating a HUMINT strategy against an issue has traditionally been to perform an open source study and assign to open sources as many primary and secondary collection responsibilities for that issue as possible. The SIGINT system, likewise, consumes a prodigious amount of open source as it beavers away, and likewise IMINT uses open sources to set in context its own divinations.

As we look to the future of more tightly coupled collection disciplines, there is every reason to suppose that open sources will provide the matrix about which the other INT's will coalesce. As I have extrapolated from present to future, I am yet humbled by Yogi Berra's commentary about the hazards of prediction, especially about the future. Allow me to reminisce about previous predictions in the open source business.

Five years ago, from a podium like this, at a conference like this, Dr. Markowitz, erstwhile Director of the Community Open Source Program Office prophesied that CIA analysts would soon have easy access to the Internet which would make information "... affordable and accessible, but [he worried that] electronic filtering hasn't progressed as far as we'd like." At that same conference, our host Mr. Steele estimated it would take US intelligence agencies five to 10 years to figure out the Internet. More colorfully, he stated that "The CIA is a dinosaur in decline, while the Internet is the future of civilisation." As it turns out, *both* gave timeless prognostications: CIA analysts are still just about to gain universal access to the Internet at large, and electronic filtering still hasn't progressed as far as we'd like. The Internet appears increasingly central to the future of civilization, and ...I leave you to decide whether CIA has proven to be a dinosaur in decline.

To close on a grander note, the ultimate test of the President's National Security Strategy is "our success in meeting the fundamental purposes set out in the preamble to the Constitution:

...provide for the common defence, promote the general Welfare, and secure the Blessings of Liberty to ourselves and our Posterity..."

And this, in turn, will be the final proof of Director Tenet's *Strategic Direction*, my supporting collection strategy, and of the open source contribution to that strategy.

REVIEW ESSAY - OPEN SOURCE INTELLIGENCE

Richard S. Friedman

From PARAMETERS, <http://carlisle-www.army.mil/usawc/parameters>

Ninety percent of intelligence comes from open sources. The other ten percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond.[1] -- Lieutenant General Sam Wilson, USA Ret. former Director, Defense Intelligence Agency

Former Ambassador to Algeria L. Craig Johnstone (presently State Department Director of Resources, Plans and Policy) recently told a Washington conference that during his assignment in Algeria, he bought and installed a satellite dish enabling him to watch CNN so he could have access to global news. He recalled:

The first week I had it running was the week of the Arab League summit in Algiers and, for whatever reason, the Department was interested in finding out whether Yasser Arafat would attend the summit. No one knew, and the day of the summit Washington was getting more frantic. We in the Embassy were banned from the summit site so there was no way we could find out whether or not Yasser Arafat would show. Finally, at about noon I was home for lunch and watching CNN when the office of the Secretary of State called. The staffer on the other end asked if there was anything at all he could tell the Secretary about Arafat's participation. And just then, on CNN I saw a live picture of Yasser Arafat arriving at the conference. "He is definitely at the conference," I reported. The staffer was ecstatic and went off to tell the Secretary. The next day I received a congratulatory phone call from the NEA bureau for pulling the rabbit out of the hat. How did you find out, they asked? The secret was mine. But I knew then and there that the business of diplomacy had changed, and that the role of embassies, how we do business in the world, also had to change.[2]

Ambassador Johnstone's story provides an example of the value of information from open sources. Allen W. Dulles, when he was Director of Central Intelligence, acknowledged to a congressional committee, "more than 80 percent of intelligence is obtained from open sources." Whether the amount of intelligence coming from open sources is 90 percent, 80 percent, or some other figure, experienced intelligence professionals agree that most *information* processed into finished *intelligence* may be available from open sources. This essay explores the significance of a trend toward increased recognition of the role of open source information and discusses what this may mean for intelligence consumers at every level.

The use of information from open sources (OSINT) for intelligence production is not a new phenomenon. Intelligence services in most nations have always made use of OSINT obtained by working with scholars in academia, debriefing business travelers and tourists, and examining foreign press and broadcast media. Intelligence prepared from sources available to the general public draws from books, periodicals, and other print publications such as catalogues, brochures, pamphlets, and advertisements. Also included are radio and television broadcasts and a more recent technological innovation, the Internet. Collectively, these are frequently referred to as open media resources.

Intelligence--information and analysis that is *not* available to the public--is prepared for use by policymakers and military leaders inside the government. Intelligence is categorized customarily according to the source from which it is obtained. Today, five sources are recognized:

- Reports from human sources (HUMINT)
- Photo imagery, including satellite
- Measurements and signature intelligence: physical attributes of intelligence targets
- Open source intelligence
- Interception of communications and other signals

While most discussions of open source intelligence seem to concentrate on intelligence collection, it is important to view intelligence trends in conjunction with developments in its traditional components. These components are:

- *Costs.* With decreasing national security budgets, government leaders are having to examine their infrastructure. As military forces become more dependent on off-the-shelf commercial technology, intelligence organizations appear headed toward greater reliance on open source intelligence.
- *Sources.* Cost-driven decisions dictate that a significant quantity of intelligence requirements can be filled by a properly designed comprehensive monitoring of open sources, either by the intelligence establishment itself or by private organizations. A particular advantage of open source intelligence is that the product can be maintained at a low level of classification required for these sources and methods. This outcome allows relatively wide dissemination and distribution when compared with material from other sources. This characteristic of open source intelligence is particularly important in coalition operations.
- *Methods.* It has been demonstrated many times that good intelligence production relies on *all-source assessment*. Traditional intelligence structures and methods have been optimized for designated core or central missions, and today many of these remain structured to meet Cold War requirements and scenarios. Current and likely future contingencies seem less likely to involve major hard military net assessments and diplomatic intelligence than was the case between 1945 and 1991. Current and future contingencies probably will continue a trend toward soft analyses of complex socioeconomic, technological, and political problems, and of issues that will include such items as international organized crime, information warfare, peacekeeping operations, and activities associated with special operations and low-intensity conflict.[3]
- *Targets.* Intelligence targets of greatest concern to US leaders have changed since the collapse of the Soviet Union, the accompanying geopolitical upheavals (such as political deterioration in the Balkans), and changes in Western perceptions of global security interests (e.g., the significance of the Middle East). Intelligence agencies must now focus their activities on a far broader range of targets and potential targets than was common in the Cold War era. Today, intelligence professionals have to be concerned with terrorism, major international crime, and arms proliferation, including programs in some areas to produce weapons of mass destruction. They have to be prepared for possible military intervention on short notice in overseas conflicts or for humanitarian relief. Some of these targets require constant scrutiny in substantial depth; for others, broad general surveillance will suffice--provided a reserve or surge capability is maintained.[4]

Although many aspects of intelligence work are changing, for the near term the preponderance of them will probably remain familiar. Today's emerging main problem is

how to deal with new and indistinct boundaries among and between intelligence organizations and functions, and increasing ambiguity in roles and missions. Any intelligence officer who has ever worked at a senior level knows that senior policymakers and government officials abhor ambiguity; they want timely, accurate intelligence. As Peter Schwartz, a recognized futurist, founding member of the Global Business Network, and author of *The Art of the Long View*, told his audience at the Colloquium on the 21st Century, "We will see not only changing rules of the game, but new games. There is an emerging competitive information marketplace in which non-state intelligence will be `cheap, fast, and out of control.'"[5]

Enthusiastic proponents of open source intelligence argue that the information revolution is transforming the bulk of any nation's intelligence requirements and reducing the need to rely upon traditional human and technical means and methods. But Robin W. Winks, distinguished Yale University historian who served in the Office of Strategic Services during World War II and in its successor, the Central Intelligence Agency, concluded, "Research and analysis are at the core of intelligence [Most] `facts' are without meaning; someone must analyze even the most easily obtained data."[6]

The emerging debate between investing in technology and developing competent analysts concerns itself basically with the value and role of open source intelligence. To understand some of the forces that are shaping the debate, we need to weigh the relative benefits of primary and secondary sources, two discrete subsidiary classes of open source material. *Primary* sources, generally taken to include print and electronic media, have always provided information of value to the intelligence community in current intelligence, indications, and warning as well as background information used by analysts in their work. What the so-called information revolution has done is to increase the ability of users to gain access and to manipulate the information, and although most intelligence managers do not believe that the number of primary sources has expanded greatly, the number of *secondary* sources has increased exponentially. To compound the analyst's problem, the objectivity and reliability of many secondary sources are often questionable. We will need more experience before we can accept expansion of secondary sources as a benefit to the management of national security.

The largest general open source collection in the world is the Library of Congress. To replace the original library, which was destroyed during the War of 1812, Congress in 1815 purchased the private library of former President Thomas Jefferson, greatly increasing the collection's size and scope. The Library of Congress now includes works in more than 450 languages and comprises more than 28 million books, periodicals, and pamphlets as well as manuscripts, maps, newspapers, music scores, microfilms, motion pictures, photographs, recordings, prints, and drawings. The library's services also include research and reference facilities, which coordinate with or amplify local and regional library resources.

There are also several thousand databases available from commercial organizations; *LEXIS/NEXIS*, *Dialog*, *Reuters*, and *The New York Times* come to mind.[7] Any discussion of contemporary open sources must now include the Internet and the World Wide Web (WWW). The World Wide Web (developed in 1989) is a collection of files, called Web sites or Web pages, identified by uniform resource locators (URLs). Computer programs called browsers retrieve these files.

The term "Internet" describes the interconnection of computer networks, particularly the global interconnection of government, education, and business computer networks, available

to the public. In early 1996, the Internet connected more than 25 million computers in more than 180 countries.[8] The Internet provides an immense quantity and variety of open source information and must be increasingly looked upon as a source for intelligence purposes.[9]

The Internet and the World Wide Web exemplify technology that is not yet mature. One hallmark of immature technology is an underlying anarchy and a potential for disinformation. In October 1938, when radio broadcasting was emerging as a reliable source of information, producer-director Orson Welles, in his weekly radio show Mercury Theater, presented a dramatization of an 1898 H. G. Wells story, *War of the Worlds*. The broadcast, which purported to be an account of an invasion of earth from outer space, created a panic in which thousands of individuals took to the streets, convinced that Martians had really invaded Earth. Orson Welles later admitted that he had never expected the radio audience to take the story so literally, and that he had learned a lesson in the effectiveness and reach of the new medium in which content was struggling to catch up to technology.

Recent examples with the Internet and its spin-offs suggest that e-mail abuses, careless gossip reported as fact, and the repeated information anarchy of cyberspace have become progressively chaotic. This does not mean that the Internet and the Web cannot be considered seriously for intelligence work, but it does mean that intelligence officers must exercise a vigilant and disciplined approach to any data or information they acquire from on-line sources.

In December 1997, senior officials from Germany, Canada, France, Italy, Japan, Britain, Russia, and the United States (the Group of Eight industrialized nations) gathered in Washington to explore the transnational nature of computerized crime, with specific attention to opportunities for criminals to exploit the Internet's legal vacuum. Among the facts presented to the officials were these:

- Almost 82 million computers worldwide are now connected, according to a Dataquest Market Research Report.
- By 2001 the number of linked computers is expected to reach 268 million.
- The FBI estimated that by 1997, the value of computer crime in the United States had reached \$10 billion per year.
- Government agencies are fertile ground for hackers; in 1995 the Pentagon was attacked by hackers 250,000 times, with a 64 percent success rate. The Department of Justice and the Central Intelligence Agency have also been hacked. And the tension over access to Iraqi weapon sites in late 1997 and early 1998 produced a surge of attempts to penetrate US Department of Defense databases.
- The San Francisco-based Computer Security Institute surveyed 536 companies or government agencies, 75 percent of which reported substantial financial losses at the hands of computer criminals.

The principal significance of these facts for the intelligence officer is that Internet sources are subject to manipulation and deception. Consequently, counterintelligence and security processing will henceforth have to include *cyberspace* during analysis.

Perhaps the greatest value to military organizations in this array of adjustments following the end of the Cold War and the proliferation of technologies is freedom from confinement to a fixed geographic site for ready access to basic unclassified references. Modern communications will free deployed military from the need to transport large quantities of

reference material (classified and unclassified) during operations. Military forces in the field can now tap into an immense quantity of information resources in near real-time. Four relevant types are:

- Basic intelligence, such as infrastructure, geography, and order of battle
- Cultural intelligence concerning the society in which the force may be required to operate
- Information of a contextual nature which relates to operational or intelligence message traffic
- Current intelligence reporting concerning the situation in the operational area

Since the quantities of information available are great and much of the information is often irrelevant, staffs of deployed units may find it difficult to use the information productively. Deployed organizations may well have to establish forward and rear intelligence activities. The threat of information warfare will have to be taken into account in planning and executing split-echelon operations.

Providing unclassified information to the general public as well as to officials is the objective of democratic governments in their declarations of open and immediate reporting. Even the tabloid press has never advocated a freedom that would deliberately compromise national security or put the lives of service members at risk, yet there can be unintended consequences from such expanded openness. The British government learned this during the 1982 Falklands campaign when a BBC reporter inadvertently revealed operational plans for what proved to be a costly assault at Goose Green by the Parachute Regiment: the enemy was listening. During Operation Desert Storm, the US government and its coalition partners would encounter other problems. While CNN was reporting directly from the theater of operations, government control of mass communications was in effect in Israel, Jordan, and Saudi Arabia, as it was in Iraq. The sites of SCUD attacks on Israel were quickly cordoned off by the authorities; media representatives were granted access only after a response had been determined by the Israeli government. The state-owned Iraqi media not only repeatedly told its citizens they were winning the struggle, but it manipulated reporting of the use of the Patriot missile against the SCUD, ensuring that CNN and others reported only what the Iraqi government wished. Coalition anti-SCUD measures soon were placed under direct control of Washington.

Intelligence consumers, government officials, and policymakers have not been complaining about a shortage of information; they are suffering from a saturation. The flood of mass-produced data now available and the ensuing overload means that collection is no longer the principal problem. The greater challenge facing intelligence organizations is analysis, consolidation, and timely dispatch of data and results to the individuals who need it. Effectiveness in this process will depend upon allocation of human resources among those responsible for analysis and others responsible for its transmission. An information management executive will consider any increase in volume as proof that information is being managed better, even more efficiently. But the information manager is not in the business of analysis, so he or she is not interested in how well or poorly the information is interpreted, or even if it contains disinformation or inaccuracy. One cannot equate increased throughput to improved situation awareness within a theater of operations.

Nevertheless, the quantitative arguments of information managers recently have become more effective than those of the intelligence community with respect to open source policy.

The last time a similar contention occurred, the proponents of technical intelligence argued that they had the key to ultimate wisdom. As the late Ray Cline, one-time Deputy Director of Intelligence at CIA and later Director of the Department of State's Intelligence and Research Bureau observed:

The technical miracle has greatly reduced the burden on the secret agent. Lives need not now be risked in gathering facts that can easily be seen by the eye of the camera. . . . Instead the agent concentrates on gathering ideas, plans, and intentions, all carried in the minds of men and to be discovered only from their talk or their written records. Nobody has yet taken a photograph of what goes on inside people's heads. *Espionage is now the guided search for the missing links of information that other sources do not reveal.* It is still an indispensable element in an increasingly complicated business.[10]

Claims of open source enthusiasts need to be examined in context. Those making extravagant claims sometimes have little vested interest in the role and value of open source materials, or even the knowledge or experience to make reliable judgments about the broader issue of multidisciplinary all-source analysis by skilled intelligence analysts.

The communications revolution is presenting intelligence organizations with a new challenge far beyond that of mass production. Like other enterprises, intelligence now faces competition from directions believed to have been impossible only a few years ago. As has been true with commerce and industry, intelligence will have to remodel its organization, form new associations, tailor or customize its products, and question its fundamental missions. So long as there are nations led by aggressive totalitarian rulers inclined toward terrorism, or there are fanatics equipped with lethal weapons, democracies will continue to need effective secret services.

NOTES

1. Reported by David Reed, "Aspiring to Spying," *The Washington Times*, 14 November 1997, Regional News, p. 1.
2. Remarks at opening session of the Conference Series on International Affairs in the 21st Century, US State Department, Washington, D.C., 18 November 1997.
3. US military operations in Somalia, Haiti, and Bosnia are examples of requirements of a different nature.
4. It is important to keep in mind an old intelligence maxim: "You can't surge HUMINT!"
5. Address, Washington, D.C., 21 October 1997.
6. Robin W. Winks, *Cloak & Gown: Scholars in the Secret War, 1939-1961* (2d ed.; New Haven, Conn.: Yale Univ. Press, 1996), p. 62.
7. One source estimates the current total to be more than 8000 such databases.
8. The Internet was initially developed in 1973 and linked computer networks at universities and laboratories in the United States. This was done for the US Defense Department's Advanced Research Projects Agency (DARPA). The project was designed to allow various

researchers to communicate directly in connection with their work. It was also developed with the idea in mind that it could provide a nuclear survivable communications system.

9. Current estimates suggest that around 30 million individuals and more than 40,000 networks are connected, numbers which appear to be increasing rapidly. The quantity of data on the Internet is huge. One estimate is total content between two and three terabytes. (A terabyte is a million megabytes.) A typical public library of some 300,000 books has about three terabytes of data. Rajiv Chandrasekaran, "In California, Creating a Web of the Past," *The Washington Post*, 22 September 1996, p. H1. An essay by James Kievit and Steven Metz, "The Internet Strategist: An Assessment of On-line Resources," *Parameters*, 26 (Summer 1996), 130-45, available on the Internet, is an excellent introduction and guide.

10. Ray Cline, "Introduction," in *The Intelligence War* (London: Salamander Press, 1984), p. 8. Emphasis added.

The Reviewer: Colonel Richard S. Friedman (USA Ret.) served in the European, African, and Middle Eastern theaters in World War II as an intelligence NCO in the Office of Strategic Services. After the war, he was commissioned from Army ROTC at the University of Virginia, where he received a law degree. He subsequently served in a variety of intelligence and special forces positions, including an assignment as the senior US intelligence officer at NATO Headquarters in Brussels. Since retiring from the Army, he has worked for the Central Intelligence Agency as a senior analyst, assistant national intelligence officer, and staff operations officer. Colonel Friedman was the lead author of *Advanced Technology Warfare* (1986) and contributed chapters to *The Intelligence War* (1984) and *U.S. War Machine* (1987). As with all *Parameters* articles and reviews, the views expressed herein are those of the author; they do not represent Department of Army policy or that of the Central Intelligence Agency or any other agency of the US government.

GREY LITERATURE

Technical Briefing by Mason H. Soule and R. Paul Ryan
From Defense Technical Information Center, <http://www.dtic.mil/>

Overview

The Intelligence Community has long taken advantage of the domain of literature offered by the large, worldwide publishing system -- that is, "normal" bookselling channels -- to identify and acquire journals, serials, newspapers, books, databases, and other types of materials that have intelligence value. Analysts combine these so-called open sources with classified materials to provide timely, dependable, and actionable intelligence information to U.S. policy makers and warfighters. Recent changes in political, economic, and even military stances around the world, as well as advances in information technology, have opened up new sources of information that are outside or not yet part of the normal publishing system. One of the Intelligence Community's major challenges today is to acquire and utilize this growing body of "grey information."

The terms "grey literature" and "grey information" are used interchangeably in this technical brief. Traditionally, grey literature denotes hardcopy books and journals, and grey information extends to other types of media. The principal distinguishing feature of grey literature or grey information is that it is outside the normal bookselling channels, which makes it relatively more difficult to identify and acquire than other open source literature. Consequently, the Intelligence Community must devise ways to simulate the awareness and document supply functions that the broader bookselling system already provides, in order to improve its coverage of this type of information. At the same time, it is important to recognize that the resources do not exist to create a duplicate system for grey information.

Scope of Grey Literature

The library science community broadly distinguishes among three kinds of literature:

- "white" or published literature (books and journals, mainly having ISBN or ISSN numbers)
- "ephemeral" literature (items of very short-lived interest such as printed airline schedules)
- "grey" literature, which falls somewhere in between the other two types.

The Intelligence Community developed a definition of grey literature to suit its particular needs, as part of its program to improve its exploitation of open source material. This definition was generated and adopted by the U.S. Government's Interagency Grey Literature Working Group (IGLWG) to support the group's charter of preparing a Grey Information Functional Plan for member agencies inside and outside the Intelligence Community. Building on a Library of Congress definition, the IGLWG distinguished grey literature from other open sources as follows:

Grey literature is foreign or domestic open source material that usually is available through specialized channels and may not enter normal channels or systems of publication, distribution, bibliographic control, or acquisition by booksellers or subscription agents

(Interagency Grey Literature Working Group, "Grey Information Functional Plan," 18 January 1995).

There are many other interpretations of what constitutes grey literature. It remains difficult to define because the boundaries between it and other open source information types vary by user group, and are fuzzy and variable in time and space. But, it is important to those tasked with acquiring this information to have as little ambiguity as possible. Accordingly, the IGLWG included a discussion of the types of information conventionally considered grey. These include, but are not limited to:

- academic papers
- committee reports
- conference papers
- corporate documents
- discussion papers
- dissertations
- government reports
- house journals
- market surveys
- newsletters
- preprints
- proceedings
- research reports
- standards
- technical reports
- theses
- trade literature
- translations
- trip reports
- working papers.

Also as an aid to collectors the IGLWG noted the major kinds of organizations that produce grey literature:

"Organizations that typically generate the largest quantities of grey literature include: research establishments (laboratories and institutes); national governments; private publishers (pressure groups/political parties); corporations; trade associations/unions; think tanks; and academia."

These clarifications are important because they provide guidance to collectors who need to know what kind of information their customers want to obtain. In summary, the key point to make regarding scope is the following. Since grey literature is not well-covered by conventional book trade channels, it is relatively more difficult to identify, acquire, process, and access than conventional open source literature. Hence, if we desire to use grey literature as a source of information, we must be prepared to accept a greater expenditure of resources to collect and process this information in comparison to other open source material.

Problems with Grey Literature

Numerous difficulties arise when analysts attempt to use grey information. Here we mention only a few major ones. First and foremost, grey literature is difficult to search for, identify, and acquire. This puts significantly more burden on the traditional "collection" stage of the intelligence cycle. For example, the only way to learn about or to acquire some trade literature and unpublished conference papers is to attend the functions at which they are made available. Collection networks must identify the event before it takes place, and coordinate attendance and literature acquisition during the event.

Second, open source information already suffers from the problem of a low signal-to-noise ratio, i.e., there are very few nuggets to be sifted from a large body of information. This problem is exacerbated in the grey literature domain because thousands of organizations generate literature, while only a fraction of these producers and their products are of interest to the Intelligence Community. The situation worsens daily as the availability of information from myriad Internet sites increases.

Third, grey literature is more difficult to process than other open source types because of its predominantly nonstandard formats. Product brochures, for example, rarely provide adequate information to allow them to be catalogued or retrieved easily. Important information, such as author, title, place and date of publication, and publisher, often is lacking from other grey literature types, as well. In addition, much grey information remains available only in hard copy. Although this is changing as Internet distribution expands, the absence of standards and keyword indexing will make it difficult to find information on this electronic forum with other than direct character matches.

Fourth, grey literature varies radically in quality since it often is unrefereed. Integrity is an issue with Internet data, as well, since electronic data are easy to alter.

Finally, foreign grey materials, which are the main interest of the Intelligence Community, are often not in English. This places additional burden on the processing system which needs human or machine translators to translate the material for the user.

Importance of Grey Literature

Key reasons for distinguishing grey literature from other open source materials lie not in the problems it generates but in the value it provides. The Intelligence Community's interest in open source literature stems from its potential to contain information of intelligence value and which may be obtained cheaper, faster, and at a lower level of classification than information acquired through other intelligence collection channels. As a subset of open source, grey information has certain other attributes, as well.

1. It can provide information that often is unavailable in published open sources. Many brochures and the information they contain never will appear in a published version.
2. It often is available on a more timely basis than conventional literature. Conference papers, for example, are available long before any follow-on, published article will appear, yet the information content of the two versions may not differ significantly.
3. It can corroborate important assertions found in other sources, which is always paramount in intelligence analysis.
4. It may have a concise, focused, and detailed content. This is particularly true of technical reports and unofficial government documents, whose information content will be greatly reduced in the published form.
5. It is becoming a common means of information exchange, particularly as personal publishing software improves and Internet access expands.

For all these reasons, grey literature must be part of an overall awareness strategy that requires a thorough search be made of all available open sources in the quest to provide answers to intelligence questions.

Federal Government Initiatives to Address Grey Literature

The successful exploitation of grey literature requires coordination and sharing of knowledge by all involved parties to reduce average unit costs of grey literature. Recognizing this, in February 1993, the Director of the Foreign Broadcast Information Service (D/FBIS) asked for IC and non-IC participation to develop a functional plan for acquiring, processing, and disseminating grey information throughout the IC. In response to that call, representatives from the Armed Forces Medical Intelligence Center (AFMIC), Army Materiel Command (AMC), Community Open Source Program Office (COSPO), Defense Intelligence Agency (DIA), Defense Technical Information Center (DTIC), Department of the Army (DA), Department of Energy (DOE), Library of Congress, National Air Intelligence Center (NAIC), National Ground Intelligence Center (NGIC), National Security Agency (NSA), National Aeronautics and Space Administration (NASA), and National Technical Information Center (NTIS), met with FBIS and other CIA Headquarters components to form the Interagency Grey Literature Working Group (IGLWG).

The Grey Information Functional Plan created by this group was approved by D/FBIS and D/COSPO and released in January, 1995. It addresses issues of acquisition, processing, and dissemination. The plan lists ten key findings that represent the basic precepts for action to make grey information available to help fulfill intelligence needs in the 1990s:

- Develop an *awareness* of the availability of grey information within or to organizations as a means of minimizing acquisition and processing costs to other agencies.
- Improve IC *cooperation and coordination* with key non-IC members that currently collect the majority of grey information materials to maximize its availability and to reduce duplicate acquisition.
- Implement *needs driven acquisition* of grey information to better manage acquisition costs.
- Identify and assign *areas of responsibility* among Government agencies to cover myriad subject areas on a worldwide basis with a dwindling resource base.
- Provide *timely notification* of the availability of relevant grey information.
- Utilize a *tiered processing approach* -- driven by user requests -- to minimize total processing costs.
- Institute *long-term storage and retrieval* systems.
- Leverage *existing U.S. Government capabilities for deposit and distribution* to reduce infrastructure costs.
- Incorporate advancements in *enabling exploitation technologies* (principally optical character recognition, machine translation, and machine-aided indexing) to improve processing.
- Employ credible *management metrics* to ensure the continuing effectiveness and efficiency of systems and processes.

The IGLWG believes that grey information can be better harnessed to satisfy intelligence needs if we can carefully implement these basic ideas among acquisition agencies and wisely use existing Government processing and distribution functions.

Members of the IGLWG have been involved in other ways to improve access to grey literature, both as individual organizations and as part of multiagency ventures. Over the past five years, first NASA and later FBIS, NAIC, DTIC, and COSPO have co-sponsored the

annual International Acquisitions Workshop to share knowledge of grey and other open source collections and acquisition methodologies among Government information specialists. Under a COSPO-funded project, NAIC developed a Grey Literature On-Line Catalog (GLOC), a database residing on the CIRC system which describes the grey literature holdings of many Government and non-Government information centers. FBIS has developed a Grey Literature Tracking Database, which describes important FBIS grey literature acquisitions as they are made available. NTIS has actively collected and made available many foreign technical reports, including a large collection of South Korean studies. The Library of Congress is working to make more Japanese grey literature available to its users. And DTIC has been working with the British Library Document Supply Centre (BLDSC) to provide access to the latter's excellent collection of conference papers and proceedings. All of these activities could benefit from the broader participation of other Government agencies on the IGLWG.

Role for Information Technologies in Processing Grey Literature

The initial summit conference and this e-journal version of the proceedings are excellent forums for the present paper because many dimensions of grey literature exploitation could benefit greatly from the infusion of Information Technologies (IT). We discuss a few ways that grey literature exploitation can be improved in the areas of acquisition, processing, dissemination, and analysis.

Acquisition

The low signal-to-noise ratio of grey literature necessitates that identification and acquisition be considered as separate steps in the collection phase, because a vacuum cleaner approach is not possible with grey literature. Acquisition instead must be demand-driven. Help is needed from the IT to relate grey literature availability to user requirements, as well as to share awareness of interagency holdings to reduce duplicate acquisitions.

Processing

Much ongoing work in the Government is aimed at improving scanning, machine-aided indexing, optical character recognition, and machine translation, which will benefit all open source exploitation. In grey literature, a tiered processing system needs to be designed so that resources commensurate with the demand for a grey literature product are expended on its processing.

Dissemination

This is not generally an issue with grey literature since its real difficulties stem from its acquisition and processing. Still, issues of copyright and electronic document dissemination are important. The size of some technical reports make them harder to transmit or store electronically, while copyright becomes a nightmare as thousands of producers must be tracked down for royalty purposes.

Use

As with processing, much work is ongoing to provide the analyst with tools to analyze digital information. Metrics are needed to evaluate the cost effectiveness of grey literature as a

marginal source of intelligence. If it is not providing significant value, then acquisition and processing methodologies must be rethought.

Conclusions

To improve analyst and information provider efforts to find grey information, we must understand what role grey information can play in solving open source intelligence issues. It is somewhat -- but not entirely -- artificial to think of grey information separately from open source since grey information is a subset of the latter. It is important, however, to know how to use grey information within this broader open source context. One must first exploit what is possible from easier-to-obtain open sources before using possibly marginal sources from the harder-to-obtain grey information domain. However, this cost reduction must be balanced against the benefit of the more timely availability of some grey literature products. Analysts must think about how grey information contributes to meeting their information needs and in what subject areas it is most advantageous or productive. Analysts then must provide feedback to the information providers who serve them.

A brief biographical notation

About Mason H. Soule: Mason Soule is a Research Scientist in the Systems Analysis and Engineering Department of the National Security Division at Battelle Memorial Institute in Columbus, Ohio. His Internet address is <mailto:soule@battelle.org>.

About R. Paul Ryan: Mr. R. Paul Ryan became the Deputy Administrator of the Defense Technical Information Center (DTIC) in July 1989. DTIC is the central source within the Department of Defense (DoD) for acquiring, storing, retrieving and disseminating scientific and technical information (STI) to support the management and conduct of DoD research, development, engineering and studies programs.

In previous positions at DTIC, Mr. Ryan was Director, Office of User Services and Marketing. He was responsible for developing and implementing a marketing program, product management program and improved user services for DTIC. The Office acts as the liaison between DTIC and its user community; manages several regional offices (Albuquerque, Boston, Dayton, Los Angeles); provides training and support to the Defense RDT&E; Online System (DROLS), and the Department of Defense Gateway Information System (DGIS); manages such special programs as the Small Business Innovation Research (SBIR) program; the Historically Black Colleges and Universities (HBCU) program and the University Research Support (URS) program; and is responsible for the annual users conference and regional meetings held each year.

APPLICATION OF OSINT

OPEN SOURCE INFORMATION

John W. Davis

Originally published in ARMY Magazine, July 1997

Imagine the horror of death by friendly fire. See the faces of a mother and father at the moment they are told their son or daughter was killed by American fire. Today, far more than bullets can cause this horrific scene. This is a new age, and there are new threats.

Information warfare is the latest theme to capture the imagination of the US Army. Force XXI, the technological army with the narrow soldier base, depends on the rapid and accurate flow of information to fuel its highly technical killing power. To protect its classified information, this army can depend on traditional security elements. This new army, however, also generates a massive amount of unclassified material that is overlooked by traditional security measures. Could this material reveal the secrets the Army hopes to protect? In the information revolution, "open source" information is the wild card of the modern battlefield. It is a form of friendly fire. The Army must protect this vulnerability through operations security.

Information - its access, use, analysis and control - is clearly a military matter. Classified information is protected by an array of security measures that are well known and practiced. But what about the literally millions of bits of unclassified personnel, logistical, operational and supply documents that Force XXI is generating? What can this information reveal and who will watch over it? What will protect this information from the silent, listening collector who is picking up the information that spews out over unsecured faxes, mail messages and telephone networks?

The Army must ask itself if this is a problem. Can the flow of information necessary to conduct operations hurt the Service? What if the unclassified material is so voluminous, so comprehensive, that it reveals the essential secrets the Army is otherwise so careful to protect?

At the beginning of World War II, some 300 British engineers died because they could not defuse the new electrical bombs dropped by the Germans over England. It took trial and error and the chance discovery of intact electrical bombs on a downed German aircraft before the technology was defeated.

Eight years earlier, in 1932, the technology for such bombs had been entered into the public records of the British patent office, yet none of the engineers knew about this open source information.

Three hundred men died while the answer they sought gathered dust in an unlikely place. Those who built the bombs that killed these men had found the information first and laid claim to it legally and openly. Had they known this, it would have been easy to convince the British people of the value of open source awareness.

An earlier example involves the Maxim gun. When asked in 1884 why Western nations had colonized almost the entire known world, the English writer Hilaire Belloc said that it was not because of their advanced civilization, greater universities or cultural advances.

No, he quipped, "Whatever happens, we have the Maxim gun, and they have not." Of course, the technology for this early machine gun and other technological information was routinely shared and sold in open contracts between "civilized" countries. In World War I this exchange of information resulted in the slaughter of an entire generation; by then all nations had access to the Maxim gun.

These stories show how open source information works. What is routinely, even inadvertently given away today could kill someone tomorrow. Information that is not tracked could later surprise the Army on the battlefield. These stories about open source information end in bloodshed. Is it inappropriate to say that the victims died from friendly fire?

Information is the lifeblood of the high-technology Force XXI. An array of information will deploy with Force XXI wherever it goes, whoever the adversary is. Unlike most of the adversaries of the United States, whose technological developments are not shared openly, much of the information about Force XXI's development is available to the entire world. For example, the Associated Press reported on a Pentagon armaments display showing soldiers with heat-sensitive night-vision sights, lightweight body armor and computer backpacks. They reported concepts about laser warplanes, seagoing missiles and more. Today there are many armaments magazines, defense sites on the Internet and newspapers reporting the business of warfare. These open sources of information are cheap, readily accessible and accurate.

Through the eyes of a western analyst, the publications are what they seem: military trade journals that cover market share, sales opportunities, competitive and joint ventures, and national acquisition goals. They are straightforward.

Graphs and computer-generated art enhance the stories and illustrate the concepts. In the photographs used, sleek missiles fly, spotless armored vehicles roll and wholesome, clean soldiers pose with the latest weaponry in pleasant pastures. There is no blood.

Consider now the reader of this same information from poorer, less industrialized, embargoed or other-wise ostracized nations. Consider also the people of para-nations, the ethnic clans, narcotics traffickers and terrorists. They see the same information in terms of life or death choices. They cannot afford technical research or development, and they cannot "comparison shop." They know they must choose wisely the first time because there may not be a second choice. For them, the only collection method may be what they can learn from open publications. The more sophisticated groups can build on information from open sources and confirm their conclusions with traditional collection methods. Their interest is far from abstract.

Several truisms must be accepted in this new world of half-wars against nontraditional adversaries. Poorer nations want to survive. In order to do so they are offered the Hobson's choice of spending what wealth they have on arms or relying on a guardian nation to arm their people. They are not interested in future sales, in market share or in the bottom line. If they do not choose correctly from the arms necessary to protect themselves, they will cease to

exist, or worse, be enslaved. Obviously, they see the world from a dramatically different perspective.

The West views military technology as a chess game. One player creates this, the opponent creates that to counter it, and so on. In this rational game of give and take, no one dies and the game goes on. Some call this the arms race, but nobody dies in a race. Such a sterile view of the industry misses the point.

Analysts of arms markets from non-Western countries or para-nations see the armaments industry differently, and arguably more clearly than Western nations do. They, like the United States, will determine their needs and do all within their power and budget to acquire those necessities. Unlike the United States, they see their existence as often nasty, brutish and short. They often feel they must confront the killer at the door, rather than the economic competitor in the pin-striped suit. It is not surprising that poorer countries decided to buy machine guns as soon as they could afford them, once they saw what happened to those who did not.

They are doing the same thing today, and have a vested interest in what is available on the arms market and in how their potential adversary will fight. What if their potential adversary is the United States?

These poorer countries want to know, simply put, how to beat the United States in battle. To be able to surprise the US military, they will try to learn more about it than the military knows about itself. They do not have the wherewithal to conduct massive technical research, so they will take any shortcut. All open sources will be exploited. Why spend the money on research and development if the final product is going to be for sale or is explained on the Internet? Why test weapons if the answers nations seek are printed in publications that cost only a few dollars each? Comparison tests will be done by those governments that see weaponry more as a commodity to be marketed than as a means of killing people.

Western powers think of long-term strategies while poorer nations wonder how to stop the immediate threat. They know they are dead if they make the wrong choices, so they research information thoroughly. If they can piece together information about the true intentions of an adversary from what they can collect on the open source market, they will do so. It may be the only source they have. These are the types of adversaries the US military will confront tomorrow.

These differing perceptions of the world - one of the rich nations, the other by poor - must be better understood. A poor man does not care about higher technology tomorrow if his weapon will surprise his enemy today. To achieve this, he may act in a way contrary to what the West considers to be in his best, rational interest. Westerners must see the world with new eyes - their potential adversary's eyes. History offers many examples.

In the 1920s, for instance, a beaten Germany, penned in by the Treaty of Versailles, entered joint ventures with Bofors Corp. of neutral Sweden. The Germans had studied the published armament policies of other European nations and had observed the soldiers occupying their country. They had studied what would win on a future battlefield, then set out to get it in any way they could.

Before World War II, Germany illegally trained its army on the land of its arch-rival, the Soviet Union. Despite open reports of Germany's illicit training, other nations were too complacent to challenge this threat. The West was thinking about long-term, rational arms races. Germany was thinking about a blitzkrieg.

In the later example, the United States was shocked when it was revealed that the Vietnamese communists had routinely spliced into U. S. telephone lines. Open communications were compromised. These were simple farmers who should not have had the capability, the United States complained. The nation did not see the world through its adversary's eyes.

Today, are the Bosnian Muslims going to rely on the United States to take action against a vengeful Serbia, or will they take their own measures? Does anyone doubt that they are devouring every statement and operational move made by the U. S. Army in the Balkans?

Every document, every communication made by the U. S. military's Balkan-deployed soldiers is subject to collection. Seemingly innocent communications could confirm or deny the fears of the many groups involved in Bosnia. How many American soldiers realize that a TDY order, supply form or logistical document could betray the military's true intentions? Open source information takes this operational release of information even farther.

Westerners may see no great loss when technology is compromised because they may never see the battle field of their work. They may think abstractly of their product as a funded program, not as something that kills someone. Their counterparts in another, less powerful country would face imprisonment or execution if they compromised hard-gathered information.

Westerners must "publish or perish." They have a "right to know" and a free and inquisitive press. Non-Western counterparts do not. The arms race fuels the West's ever expanding market and the information-rich marketing ethic that advertises it. The military must create policies that protect all its information - even the unclassified - because, in this new world, information that kills soldiers is a commodity available for sale.

Operations security, a process of securing this unclassified information, can protect Force XXI. The security process is simple. Each element of the Army must ask itself, "What is it that I must protect, or else I'll fail in my mission?" The answer is that critical information must be protected, as Sun Tsu noticed so long ago. Not everything that can compromise a mission is classified.

Next, the collection threat to this information must be studied. Soldiers must consider who wants what they have. Here, the intelligence community can provide assistance. The collection capability could be a highly sophisticated process or a hacker who can read the Army's e-mail. In weighing the threat to the critical information, the answer to the next question, "Is the Army vulnerable?" may be surprising. Even units with 100 percent traditional security of their classified information have been compromised by a hemorrhage of unclassified data. Unit leaders did not tell their soldiers what was critical to protect, and soldiers did not control bar talk, telephone talk or what went out over the wire, much less what went into the trash. After the risks are weighed, such as collection capabilities and reaction times, countermeasures must be decided on.

The Army must communicate to accomplish any mission, but it has to remain aware of the unseen listener. Soldiers must know what an adversary can do. To survive, other countries will read everything the Army writes and listen to any conversation they can. The Army has to see itself as others see it.

Once they learned that the Viet Cong had made tiny mines from discarded C-ration cans, soldiers stopped leaving cans uncontrolled. Now, the Army should do no less with its open source information.

NEW RISKS OF CRISIS - FRESH PERSPECTIVES FROM OPEN SOURCE

Dr Brian Rotheray, BBC Monitoring – 2001
Copyright BBC, <http://www.monitor.bbc.co.uk/>

OPEN SOURCE

An early British open-source handbook tells the story of a general sent to subdue an island. This island had recently been partially occupied and was in revolt. The general succeeded. He was an imaginative and decisive officer and he made extensive use of the various forms of intelligence.

He sent out ships to chart the island's coast and identify its harbours and waterways - *naval intelligence*. He surveyed the interior - *mapping* and *imagery*. He studied the weapons of the local rebels and their tactics and devised his own methods to counter them - *military intelligence*. When it suited, he made deliberately slow progress through the country, allowing his reputation to go ahead of him - *media spin*. He investigated the state of agriculture and industry, identified mineral deposits and mining potential and established that the country was worth occupying - *economic intelligence*. He had reported to him the speeches of rebel leaders and so heard their arguments and knew what they said about him - *political intelligence* and *open source*. (Some speeches are fully texted in the book.) And he studied the locals. He found out about their languages and religion and character and "he listened to the experts" - *cultural intelligence*. He learned what made the people tick, particularly that "little was accomplished by force if injustice followed", and after winning he governed accordingly.

This is not a recent book and it is about the British, not by them. It is by the historian Tacitus and is the biography of his father-in-law Gaius Julius Agricola, who subdued Britain for the Romans two thousand years ago. Plenty of sand has run through the glass since then, but the same basic ideas apply.

Monitoring the media is as old the media. Former German Chancellor Helmut Schmidt is supposed to have said that he got more out of reading the *Neue Zuericher Zeitung* - a Swiss daily newspaper - than out of all his intelligence briefings. Part of the humour of this is that the *Neue Zuericher* looks like an old fashioned "intelligencer" with the style of an eighteenth-century broadsheet.

All countries and governments practise media monitoring in some form or another. From the Japanese embassy in London monitoring the UK press, through the mighty German Chancellor's press office, via companies that track mentions of toothpaste manufacturers - and the like - on local music stations, to the great spin-doctoring concerns that influence every move a politician makes. Governments, parties, interest groups, transnationals - they are all at it.

The BBC is a major broadcaster domestically within the United Kingdom and internationally. It employs around 22,000 staff, runs a number of national and international television channels, five national and around 40 local radio channels. In addition, BBC World Service radio broadcasts in 40 languages and has around 150 million listeners. There is also a major

commitment to Internet services, including BBC News online – one of the world’s best-known.

Since 1939, the BBC has found it worthwhile to monitor other broadcasters – other media – around the world and it continues to support a unit to do this. The BBC does this to understand its markets and competition and to help it report the news to those markets.

The BBC also sees its monitoring service as a national asset supporting British interests. Our reporting helps inform a British and world public and deepens public understanding about what is going on in the world and why. It is a service to the British government, civil service and institutions. In effect BBC Monitoring sees open source media reporting as helping a number of communities of interest:

- the diplomatic community – and the wider community of those interested in foreign affairs;
- the defence and intelligence – and law-enforcement – communities;
- the fourth estate – broadcasters and other media – and through them the British and international public;
- the legislature – parliament and its members;
- also the educational and the business communities;
- and what is described in Britain as “joined-up government” – the bits that aim to make the individual elements act as a coherent whole. In practice that means the Prime Minister’s own offices.

All these “communities”, these types of organisation, can benefit from knowing what is appearing in the media around the world. And there are three types of benefit that an organisation like BBC Monitoring can offer:

1. Individual reports - many hundreds a day about what is happening in the world - information
2. A picture of what people and the media in a country or region are saying - opinion
3. Knowledge management – assistance in wading through millions of words in numerous languages from almost innumerable media sources and making some sense out of them

The valued-added help in data **navigation** comes from:

- knowledge of countries, languages and cultures,
- knowledge of the sources and media environment
- knowledge of the customer's needs and tools, as well as human skill to deliver the right material to suit the right function in a given situation.

BBC Monitoring's aim is to provide sustained global coverage, maintaining a wide overview of foreign media source and monitoring the key ones.

This means not **just radio and television**, but also news **agencies** and the **press** and the **Internet**.

Working in partnership with FBIS, BBC Monitoring offers output from the monitoring of around 3,000 sources in 150 countries and from 100 languages. What is offered is the product of a high level of skill and understanding.

BBC Monitoring provides global coverage through its close partnership with FBIS - the US Foreign Broadcast Information Service. The partnership works through a division of coverage and by working to similar operational and editorial standards. Each partner passes the other its monitored output - the transcripts; each partner turns these transcripts into products and services for its respective customers.

FBIS provides coverage of the Far East and Latin America. The partners share coverage of Africa, the Middle East and Europe. BBC Monitoring majors in the FSU and Central Asia. Both partners maintain a string of monitoring operations to cover their areas.

BBC Monitoring's key trademark is that it tells you "**the words as spoken**" - exactly what a television service is reporting, exactly what a minister says in an interview, exactly what a treaty contains.

Around 800 reports are issued each day. Reports like these can be accessed through Internet databases, profiled directly to end-users or fed into user organisations' intranets.

Thousands of words and more than words. Also pictures, sound, information about the make up of governments and other official organisations.

It is important that this is also a service - not just a machine. At the highest level of service the users get desk-to-desk contact with the monitors who know the target countries and the topical issues.

BBC Monitoring is aiming to provide effective open source intelligence - to help cover the needs of different functions in different situations at different times that add up to a strikingly coherent overall need. Our target: to collect **the right information**, make it **plain**, and deliver it to the **right place** at the **right time**. In conclusion, a short open source "entertainment" from the archives:

DON'T IGNORE THE OBVIOUS [with apologies to James Thurber]

The goose family - father goose, mother goose and daughter goose - is sitting at home minding its business. Suddenly there is a ring at the door.

"Aha," says daughter goose. "No doubt it is a young gentleman caller for me!"

"Forget it, honey," says father goose. "I'm expecting a brush salesman come to sell me a brush. I'll open up"

Mother goose - more careful - looks out the window and sees a large, hungry-looking wolf with sharp teeth and a bushy tail

"It's a wolf," she says. "Got wolf written all over him. Teeth and a big tail. Don't open the door."

“Don't be silly, honey,” says father goose, not bothering to look. “There's no wolf activity round here. There's a bunch of guys working undercover on wolves. They'd warn us if there was anything going down. It's the brush salesman What you think are teeth are its business cards. What you think is the tail is my brush. ”

So he opened the door - and the wolf ate him up.

The moral: What's open source for the goose may not be open source for the gander.

SECRETS FOR SALE: **HOW COMMERCIAL SATELLITE** **IMAGERY WILL CHANGE THE WORLD**

Yahya A. Dehqanzada and Ann M. Florini

Excerpts from “Secrets for Sale: How Commercial Satellite Imagery Will Change the World” reprinted by permission of the publisher (Washington, D.C.: Carnegie Endowment for International Peace, 2000)

EXECUTIVE SUMMARY

By the year 2003 at least eleven private companies from five different countries expect to have high-resolution commercial remote sensing satellites in orbit. These new satellites have capabilities approaching those of military spy satellites, but with one key difference: their images will generally be available to anyone able to pay for them. This new technology raises a host of policy concerns with which governments, business executives, and analysts around the world are just beginning to grapple. This monograph, inspired by the discussions at a recent conference of the Carnegie Endowment for International Peace, addresses those policy concerns(1).

Key conclusions are that:

Increased access to high-resolution satellite imagery will shift power from the former holders of secrets to the newly informed. Governments that previously had limited or no access to satellite imagery can for the first time see what elite states have observed from the skies for many years. In addition, commercial satellite imagery will provide an independent source of information to groups in civil society. Both state and non-state actors will employ satellite imagery to monitor and sometimes publicize the activities of various countries and corporations.

High-resolution satellite imagery has both beneficial and malign applications. It can significantly enhance the ability of governmental and nongovernmental organizations to respond quickly to sudden humanitarian emergencies such as in Somalia and Iraq, document and publicize large-scale humanitarian atrocities such as those witnessed in Kosovo and Rwanda, help control environmental problems ranging from impending droughts to deforestation, monitor compliance with international agreements, and assist in managing international disputes before they escalate to full-scale interstate wars. But abundance of information does not guarantee benevolent uses. State and non-state actors could employ remote sensing imagery to conduct industrial espionage, collect intelligence, plan terrorist attacks, or mount offensive military operations.

Attempts to control access to high resolution satellite imagery are bound to fail. Since the end of the cold war, technological progress, coupled with a greater appreciation for the military, civilian, and commercial utility of high-resolution satellite data, has persuaded governments and corporations in virtually every region of the world to invest in indigenous remote sensing industries. As a result, both the satellite technology and the necessary support infrastructure have become global. It is unlikely that any one country, regardless of its size or market share, can by itself curb access to high-resolution satellite imagery. And because of the large number and varied political agendas of the countries that will operate various

satellites (Canada, France, India, Israel, Russia, the United States, and possibly China), multilateral agreements on control seem elusive. Governments need to accept this new era of mutual assured observation, take advantage of its positive effects, and find ways to manage its negative consequences.

Commercially available high-resolution satellite imagery will trigger the development of more robust denial and deception and antisatellite countermeasures. Widely available high-resolution satellite imagery will undoubtedly compel governments to develop effective means for keeping their secrets hidden. Many states, especially those with regional adversaries, will invest heavily in denial and deception and antisatellite countermeasures. Such a development could have serious implications for confidence-building and crisis management among mutually vulnerable states.

Expected gains from commercial high-resolution satellite imagery may be exaggerated. Satellite imagery is only one source of data among many. While it can detect large-scale troop movements, mass graves, and deforestation, it cannot reveal what those troops' intentions are, who is buried in the mass graves, or how deforestation can be stopped. Complementary data are necessary to turn satellite imagery into usable information.

Good training for imagery analysts is essential. Satellite imagery can be difficult to interpret. It takes years before an analyst gains the experience and expertise necessary to be able to derive useful information from gigabytes of transmitted data. Junior analysts are wrong far more often than they are right. It is essential that imagery analysts go through extensive training not only at the beginning of their careers, but also every time they shift the focus of their work—analysts who specialize in interpreting and analyzing the activities of ground forces cannot overnight become experts on nuclear testing or environmental issues.

INTRODUCTION

Over the next five years, at least five private companies around the world plan to launch commercial remote sensing satellites able to detect objects as small as one meter across. That level of detail is not as good as that of current government-controlled spy satellites, which by most accounts can achieve a resolution of just a few centimeters, but it is getting close. One key difference renders the commercial satellites far more interesting and possibly far more destabilizing than the state-owned spy satellites: the operators of these systems are not going to hide the imagery in the bowels of intelligence agencies, but are going to sell it to anyone able and willing to pay. The new commercial satellites will make it possible for the buyers of satellite imagery to, among other things, tell the difference between trucks and tanks, expose movements of large groups such as troops or refugees, and determine the probable location of natural resources.

Whether this increased access to imagery amounts to a positive or negative development depends on who chooses to use it and how. On the plus side, governments, international organizations, and nongovernmental groups may find it easier to respond quickly to sudden movements of refugees, document and publicize large-scale humanitarian atrocities, monitor environmental degradation, or manage international disputes before they escalate to full-scale interstate wars. The United Nations, for example, is looking into the possibility that satellite imagery could significantly help curtail drug trafficking and narcotics production over the next ten years. Similarly, the International Atomic Energy Agency is studying the utility of

commercial high-resolution satellite imagery for monitoring state compliance with international arms control agreements.

But there is no way to guarantee benevolent uses. Governments, corporations, and even small groups of individuals could use commercial satellite imagery to collect intelligence, conduct industrial espionage, plan terrorist attacks, or mount offensive military operations. Even when intentions are good, it can be remarkably difficult to derive accurate and useful information from the heaps of transmitted data. The media, for one, have already made major mistakes, misinterpreting images and misidentifying objects, including the number of reactors on fire during the Chernobyl nuclear accident in 1986 and the location of the Indian nuclear test sites just last year.

Such bloopers notwithstanding, the new satellite imagery will provide many people with information to which they never before had access. The implications for national sovereignty, international peace and security, the ability of corporations to keep proprietary information secret, and the balance of power among the former holders of information (a few industrialized states) and the newly informed (other governments and global civil society) are serious. Undoubtedly states will attempt to maintain tight controls over this new source of information. Whether their efforts will succeed remains to be seen.

In short, the new form of transparency brought about by the advent of high-resolution commercial satellites raises a host of pressing questions. Does it portend an age of peace and stability, or does it create vulnerabilities that will make the world more unstable and violent? What contributions can emerging remote-sensing technologies make to the fields of news reporting, humanitarian relief, environmental protection, and international security? What policies could the United States and other countries adopt to secure the benefits of growing international transparency while limiting its potential negative consequences?

The Technology of Remote Sensing

An analysis of the implications of the new satellites requires a basic understanding of what the various existing and future systems can see and do, what the jargon used in the remote sensing field means, and what types of sensors exist.

Perhaps the best-known concept is that of *spatial resolution*. Spatial resolution refers to the size of the objects on the ground that the satellite sensor is able to detect. A satellite image is a mosaic. A sensor applies one value (a shade of grey or color) to each square of the mosaic. For a satellite with 1-meter resolution, each square in the mosaic corresponds to one square meter of ground area, while 10-meter resolution corresponds to ten square meters on the ground—a difference of a factor of 100 (see image on page 26).

At present, civilian and commercial satellites carry one of three types of sensors: film, electro-optical, and synthetic aperture radar (SAR).

Film sensors take actual photographs, with the film returned to Earth either by retrieving ejected film capsules or by recovering the entire satellite. Both U.S. and Soviet spy satellites started off using film, and many Russian satellites still do. Film provides good high-resolution imagery but has two real drawbacks. It can be slow, since it usually has to be physically retrieved and developed, and the satellite becomes useless once it runs out of film, a characteristic that requires frequent launches of new satellites.

Electro-optical sensors overcome these disadvantages. They measure the electromagnetic radiation reflected off or emitted by objects on the Earth's surface, creating digital images of ground features that are then transmitted to receiving stations on Earth in a matter of minutes. However, these systems, like film, do not produce their own signals and therefore depend on other sources of energy such as the sun to illuminate the objects being observed. This characteristic constrains the use of both types of systems to daylight hours and favorable conditions. Bad weather or smoke can severely limit what these systems can see.

There are three different types of electro-optical sensors. Panchromatic sensors detect energy reflectance in only one band of the electromagnetic spectrum and thus produce black-and-white imagery. Multispectral sensors can measure electromagnetic reflectance in several different color bands—usually three to seven—and so produce color images. Hyperspectral sensors, through a similar technique, image objects using many different spectral bands. The ability of hyperspectral sensors to distinguish tens and sometimes hundreds of different shades of color allows them to provide a great deal of information about the composition of features on the Earth's surface not discernible by either panchromatic or multispectral instruments.

With synthetic aperture radar sensors, the systems transmit a signal in the microwave part of the spectrum to the Earth's surface and then detect the characteristics of the return signal after it reflects off objects on the surface. Because radar satellites emit their own signals and operate in longer wavelengths than electro-optical systems, their operations are not limited to daylight hours. Synthetic aperture radar sensors can image any spot on Earth day or night, in any weather, through clouds and smoke. As with the electro-optical systems, they produce digital data that can be downloaded to ground receiving stations moments after the images are collected.

APPLICATIONS OF EMERGING REMOTE SENSING CAPABILITIES

In 1858 the French photographer Gaspard-Felix Tournachon (popularly known as Nadar) pioneered the field of remote sensing when he took the world's first aerial photograph of Paris from his gas balloon, *Le Géant*, 250 feet above the ground. Two years later Nadar found himself taking aerial pictures of enemy troop movements during the 1870 Franco-Prussian war.⁽²⁾ What had started as one man's desire to capture the imagination of the world through the lens of a camera suddenly found novel applications in the bloody field of interstate warfare.

Since those early days, many more applications have been discovered for remote sensing data. Although the age of easy access to timely high-resolution satellite imagery is just now dawning, for several decades imagery has been available from aircraft and even (at lower resolutions) from government-operated satellites (see Chapter Three and Appendix B). Over the past thirty years, governments, corporations, and nongovernmental organizations have used aerial and space-based imagery platforms to, among other things, collect intelligence, execute military operations, plan development projects, and monitor the environment. It seems likely that as the availability of high-resolution imagery grows, and especially if the prices drop, governments and non-state actors will find new arenas where remote sensing data can be of value.

Although a discussion of the full range of applications for remote sensing data is beyond the scope of this monograph, the brief overview that follows provides a glimpse of the multifaceted significance of this powerful form of global transparency.

Security Applications

Of all the applications of commercial high-resolution satellite imagery, the most controversial and the most lucrative are its security applications.(3) In the short term, nearly half the sales of high-resolution imagery will be made to defense and intelligence organizations worldwide.

High-resolution commercial satellite imagery can help governments, especially those with no indigenous imagery collection capabilities, monitor the activities of neighbors and regional adversaries and expose violations of international norms and treaties. In August 1987, for example, the German foreign intelligence service, the Bundesnachrichten Dienst, used 10-meter resolution SPOT imagery to publicize the construction of a chemical warfare production facility near Rabta, Libya.(4) Space-based reconnaissance is particularly well suited for this type of intelligence collection because it is sanctioned under international law and is considerably less intrusive than either aerial or on-ground surveillance. An added advantage of commercial satellite imagery is that it can be shared. Whereas government officials closely guard spy satellite images to conceal the technical capabilities of national reconnaissance systems, commercial imagery can easily be shared with foreign governments and international organizations, a considerable advantage in multilateral operations such as those in Iraq, Bosnia, or Kosovo.

In addition to intelligence collection, high-resolution commercial satellite imagery can help identify enemy vulnerabilities, plan military operations, assess strike effectiveness, and prioritize targets for follow-up missions. There is some evidence that the Iraqi military may

Bomb damage assessment photos released by the U.S. Department of Defense on December 17, 1998, of the Baghdad Directorate of Military Intelligence Headquarters.



have used 10-meter resolution SPOT satellite photographs for attack planning and post-attack assessments both during the eight-year Iran-Iraq war and prior to the invasion of Kuwait in August 1990.(5) SPOT and Landsat imagery later helped the allied forces expel the Iraqi troops from Kuwait.(6)

Technological advances are likely to increase the demand for commercial satellite imagery. With the launch of the world's first hyperspectral sensors on board the OrbView 4, Naval

EarthMap Observer, and Aries satellites, all of which are scheduled to begin operations within the next three years, security agencies worldwide will have access to richer data for intelligence gathering and military planning. Hyperspectral imagery can detect any type of camouflage that is not natural and growing. Green plastic and foliage have unique spectral signatures that are easily distinguishable from living vegetation. Military planners can use such information to design and carry out precision strikes against concealed high-value targets. In addition, hyperspectral sensors may be able to identify high concentrations of different chemicals in the soil.(7) It may be possible to employ these sensors to monitor, document, and publicize the production and use of chemical weapons in different parts of the world.

There is no reason to believe that the demand for commercial satellite imagery for intelligence collection and military planning will abate any time in the near future. As long as armed conflicts occur, government demand for remote sensing data is likely to remain high, regardless of what happens to the prices of satellite imagery. If anything, with the launch of new systems with better spatial and spectral resolutions and shorter turnaround times, demand will continue to grow.

Humanitarian Application

On August 10, 1995, Madeleine K. Albright, at the time the United States' chief delegate to the United Nations, called the attention of the international community to atrocities committed by Bosnian Serbs against Bosnian Muslims after the fall of the UN "safe area" in Srebrenica.(8) Amb. Albright presented the UN Security Council with American spy satellite images that showed people herded into a soccer field at Nova Kasaba the previous July 13 and 14. Imagery collected several days later revealed an empty stadium but mounds of freshly dug earth in the nearby field. After the end of hostilities, war crimes investigators exhumed the graves and recovered the bodies of dozens of Bosnian Muslims(9).

The 1995 incident unveiled to the world the power of satellite imagery in monitoring, documenting, and, possibly, deterring large-scale humanitarian crises. On April 1, 1999, as a new chapter of Serbian aggression was being written, this time against Kosovar Albanians, members of ten human rights and religious organizations gathered at the National Press Club in Washington, D.C., to call upon the Clinton administration to "immediately provide the International Criminal Tribunal for the Former Yugoslavia with all available intelligence information that reveals evidence of atrocities in Kosovo, specifically imagery collected by satellites, aircraft, and unmanned air vehicles."(10) Responding to such demands, the United States and the North Atlantic Treaty Organization (NATO) released numerous satellite images of mass graves in different parts of Kosovo, including Glodane, Velika Krusa, Pusto Selo, Glogovac, and Izbica.

The flood of spy satellite imagery made available to the public during the Kosovo crisis was unprecedented. It is not clear, however, whether the United States and its NATO allies will be so open again. Publicizing the egregious acts of the Serbian forces in Kosovo clearly served the political objectives of the Clinton administration, which was trying to win the support of the international community in general and the American public in particular. It seems doubtful that a future U.S. administration would be as forthcoming if releasing spy satellite imagery meant having to take action against states with close ties to the United States or having to consider undertaking a major engagement in less strategically significant parts of the world, such as Rwanda, Sudan, or Afghanistan.

The advent of commercial high-resolution satellites will guarantee that in the future the Milosovics of the world will not be able to carry out their sinister plans unobserved. Satellites can document events in the remotest corners of the world, or in areas where security concerns limit access to international observers and media groups. Such information can later be used to publicize humanitarian emergencies and possibly punish the perpetrators of humanitarian crimes. Commercial satellite operators are generally not restrained by the sort of political constraints that often muzzle the response of state governments. Whereas states may refrain from publicizing acts of humanitarian violence in other friendly countries or in countries where they do not wish to get involved, commercial satellite operators will readily market such imagery to a host of media and human rights groups. Such widely available satellite imagery might deter states from committing large-scale violence against ethnic minorities and might compel the international community to take action once such acts of violence are committed.

United States surveillance photograph in a handout presented by the chief U.S. delegate to the United Nations on August 10, 1995, showing alleged mass graves in Nova Kasaba, Bosnia (later found to contain bodies of Muslim civilians massacred by the Bosnian Serbs).



Aerial imagery from a NATO handout released on April 17, 1999, showing what NATO described as new graves near Izbica, Kosovo.



High-resolution satellite imagery can also provide state and non-state actors with valuable information on how to respond to humanitarian emergencies. Large refugee movements can be tracked using imagery with a resolution of 1 meter or better. Such imagery could help determine the direction of refugee flows, the size of different refugee pockets, ground surface

features, and the resources available to humanitarian response teams. Employing high-resolution satellite imagery to plan relief operations could significantly improve the ability of various groups to alleviate human suffering in the wake of large-scale humanitarian emergencies.

Environmental Applications

For the past twenty-seven years, low and medium-resolution civilian satellites have provided invaluable data on the status of the Earth's temperature, land cover, water bodies, and atmosphere.(11) For example, satellite imagery has allowed scientists to monitor and document the depletion of the ozone layer over the South Pole, the shrinking of the Aral Sea

Five-meter-resolution imagery taken by the Indian Remote Sensing satellite (IRS-1D) on May 8, 1999, depicting the destruction left behind in the wake of a powerful tornado near Oklahoma City.



in the former Soviet Union, and the rate of loss of the tropical rainforests in the Amazon basin. In addition, remote sensing systems have at times played a central role in managing serious environmental emergencies. After the 1990-1991 Persian Gulf War, the thermal-infrared sensors on board the Landsat 4 satellite provided firefighters with critical information on the exact location of some 529 oil fires in liberated Kuwait.(12) More recently, the Canadian RADARSAT-1 system helped avert a potential disaster by providing timely information on the size and direction of a large oil slick near the water intake pipes of a nuclear power plant on the coast of Japan.

As these examples illustrate, remote sensing systems have for decades satisfied many of the data needs of various government agencies, scientists, and environmentalists. In the future, emerging commercial satellites with higher spatial and better spectral resolutions will supplement and complement (but not replace) existing environmental monitoring capabilities. The primary reason is that most environmental changes are slow, evolving processes that take place across extensive tracts of Earth over lengthy periods. To monitor and document long-term environmental change, scientists need continuous coverage of vast regions. The existing high price of commercial satellite imagery makes it virtually impossible for anyone except the most affluent environmental organizations to purchase large quantities of high-resolution satellite imagery. Whereas the U.S. government provides Landsat 7 pictures for \$475 to \$600 per scene, commercial satellite operators routinely charge \$4,400 for a comparable product. Although these prices may decline as the number of commercial systems in operation increases, that drop is unlikely any time soon, given that the commercial satellite companies are trying to recoup investments on the order of hundreds of millions of dollars.

While existing civilian satellites have a comparative advantage in long-term, wide-area monitoring of the environment, emerging commercial satellites seem to be particularly well suited for periodic assessments of areas of greatest concern. Possible environmental applications of emerging commercial satellites include: studying the impact of land development and energy exploration on wilderness areas, developing more complete wetland inventories, monitoring the health of vegetation in all regions of the world but particularly in remote or inaccessible areas, and detecting toxic discharges from mines and production facilities.

Governments, corporations, and conservation groups are slowly beginning to understand the immense potential of remote sensing data for environmental monitoring and are taking steps to better incorporate such data into their decision making. In 1995 the U.S. Environmental Protection Agency (EPA) conducted a study on the possibility of employing hyperspectral sensors to monitor toxic runoffs from abandoned mines. It conducted the experiment at the CalGulch Mine Superfund site in Leadville, Colorado, which is home to hundreds of relict gold, silver, lead, and zinc mines suspected of contributing acid drainage and heavy metals to downstream supplies of drinking water. Using NASA's aerial hyperspectral sensor, the Airborne Visible and Infra-Red Imaging Spectrometer (AVIRIS), the EPA was able to study the site while saving approximately "80 percent of the time and cost of traditional ground-based analysis."⁽¹³⁾ After the success of the CalGulch Mine experiment, the EPA launched an Advanced Measurement Initiative (AMI) to accelerate the adoption and application of remote sensing and other technologies that could provide more timely, accurate, and cost-effective environmental monitoring data. Under the initiative, the EPA has undertaken two new projects involving hyperspectral sensors to monitor the presence of jarosite (a mineral that can contribute to acid drainage and the release of heavy metals into the environment) in the Ray copper mines in Arizona, and to measure the concentration of suspended minerals, chlorophyll, and dissolved organic carbon in the surface waters of the Neuse River in North Carolina. The results of both studies were to be released at the end of 1999.

Mindful of the bad publicity associated with lax environmental practices, a number of multinational corporations have also begun using remote sensing technologies to police their own activities. The Texas oil giant, Texaco, for example, developed an aerial hyperspectral sensor called Texaco Energy and Environmental Multispectral Imaging Spectrometer (TEEMS) to help it pursue environmentally sound policies. Once fully operational, this imaging capability will allow Texaco to, among other things, establish environmental baselines prior to commencing exploration, conduct fracture analysis on its vast network of pipelines, identify oil seeps and oil spills, and, when necessary, take action to minimize and reverse damage done to the environment.

The use of remote sensing data for environmental monitoring is not limited to state governments and large corporations. Environmental nongovernmental organizations have for years made extensive use of existing relatively low-resolution imagery to monitor enforcement of the U.S. Endangered Species Act, document the destruction of coral reefs around the world, and generate plans for ecosystem management.⁽¹⁴⁾ As more sophisticated commercial remote sensing systems become available, and especially if the prices drop, it can be expected that environmental groups will expand their activities, monitoring compliance with existing environmental standards and publicizing violations.

Media Uses of Satellite Imagery

On Saturday, April 26, 1986, two explosions destroyed Unit 4 of the Chernobyl nuclear power plant in Ukraine and released 100 million curies of radionuclides into the environment.(15) Hoping to keep the incident secret, the Soviet government immediately sealed off a 100- mile radius around the stricken reactor and banned all foreign travel to Kiev, the largest city nearest the site of the accident.(16) Two days later, as radioactive clouds began setting off radiation alarms throughout Europe, the Soviet news agency Tass confirmed Western suspicions by disclosing that one of its atomic reactors had indeed been damaged.

Within hours of the announcement the United States' top-secret spy satellite, Keyhole (KH-11), began collecting imagery of the Chernobyl power station. By Tuesday, April 29, KH-11 photos were in the hands of U.S. policy makers in Washington, D.C. But this time government officials did not have exclusive access to satellite imagery. Less than twenty-four hours after Keyhole images reached the White House, the American Broadcasting Company (ABC) aired medium-resolution Landsat images of the blazing nuclear reactor.(17) Shortly thereafter, a number of media organizations began broadcasting higher resolution SPOT images of the Chernobyl power plant.

In the decade and a half since the Chernobyl accident, the use of satellite photos by news organizations has increased significantly. Despite the relatively low resolution of publicly available satellite systems, media groups have employed remote sensing technology to report on important events such as the military buildup in the former Soviet Union, the Persian Gulf War, weapons proliferation in the third world, the U.S. assault on Osama bin Laden's hideaway in Afghanistan, the devastation left by a tornado that swept through Oklahoma City, the nuclear tests in India and Pakistan, and, more recently, the humanitarian atrocities in Kosovo.

With the advent of commercial high-resolution satellites, the use of remote sensing imagery by media groups is likely to grow. Imagery, even relatively fuzzy commercial satellite photos, allows news agencies to convey important information visually to their audiences. More important, satellites can go places that are otherwise inaccessible to media groups. These two features alone will ensure the continued use of satellite imagery by news organizations for years to come.

Business Applications

The full range of commercial applications for satellite imagery is not yet known. A number of factors, including cost, timeliness, and spectral as well as spatial resolution, will ultimately determine how narrowly or broadly remote sensing imagery is employed. However, several commercial applications of satellite imagery are worth noting here.

Satellite imagery has important applications in map making. While 95 percent of the world's land mass is mapped at a scale of 1:250,000, only 33 percent is mapped at 1:25,000. Less than 10 percent of Africa and South America and less than 20 percent of Asia and Australia are mapped at the higher scale. In many cases the maps available at the higher scale are outdated or incomplete. Emerging high-resolution commercial satellites will significantly improve both the scale and quality of maps of the more remote and less developed regions of the world.

Another major commercial application of high-resolution satellite imagery is in the field of agricultural management. Agriculture is a volatile field with pronounced effects on the economic well-being and political stability of nations. Satellite imagery can help take some of the unpredictability out of this important sector. Multispectral and hyperspectral sensors are well suited to predicting crop yields, detecting crop disease and insect infestation, and monitoring thermal stress.(18) Satellite imagery can be used to prepare detailed maps of agricultural fields to determine the best seeding and irrigation patterns, as well as the optimum amounts of fertilizer and pesticides needed to obtain higher crop yields.

Satellite imagery can also help pinpoint the probable location of nonrenewable natural resources, a capability that can dramatically reduce the economic risks of exploration. Radar imagery, for example, has for years helped oil companies identify new offshore oil reserves. According to Roger Mitchell of the Earth Satellite Corporation, nearly 80 percent of offshore oil exploration starts by searching for oil seeps.(19) Oil's viscosity retards wave formation, causing a "calm spot" on the ocean surface. Radar satellites can detect these calm spots and analyze their suitability for future exploration.

Similarly, hyperspectral sensors can inspect the Earth's surface for unique spectral signatures associated with particular resources. Once a signature is detected, mining companies can begin exploration activities with much greater confidence. In the next few years, hyperspectral sensors may revolutionize exploration for natural resources in all corners of the world. Unlike the traditional methods, satellites can image any region on Earth regardless of its accessibility and can provide accurate information at a significantly lower cost. However, for hyperspectral imagery to be useful, additional research is needed to compile a more thorough library of the spectral signatures associated with different natural resources.

Urban planners can also use satellite imagery to improve efficiency and reduce costs. Houses, water tanks, canals, sidewalks, pavements, and parking lots are easily distinguishable on high-resolution satellite imagery. City officials can use such information to plan new development projects and design improved networks of public utilities. Remote sensing data can provide engineers and construction companies with valuable information on soil composition and structural morphology before substantial investments are made.

Finally, remote sensing data provide corporations new opportunities to spy on their competitors. A comparison of archived and more recent satellite imagery can reveal important information about the production capacity of rival companies at dispersed locations around the world. For example, high-resolution satellite imagery can reveal new construction, new types of shipping containers on loading docks, or an increase in the number of rail cars used to distribute products.(20) Although traditionally observers on the ground have obtained such information, commercial satellite imagery may prove to be more cost-effective and significantly less intrusive.

Competitive Intelligence or Industrial Espionage?

There has never been a ruling on the legality of space-based imagery for competitive intelligence. The only relevant case, which may form the basis for all future litigation, dates back to 1970. In *E.I. du Pont de Nemours & Co., Inc. v. Christopher*, DuPont sued the Christopher brothers for taking aerial pictures of its Texas plant while the plant was under construction to learn DuPont's new process for methanol production (Fred Wergeles, "Commercial Satellite Imagery: New Opportunities for Competitive Intelligence,"

Competitive Intelligence Magazine). In this case, the court ruled in DuPont's favor, citing the steps taken by the company to protect its trade secrets and the improper means used by the Christopher brothers to uncover those secrets.

The advent of commercial high-resolution satellite imagery may have a profound impact on how cases involving remote sensing imagery are adjudicated in the future. In *DuPont* the court adjudged the actions of the Christophers to be improper primarily because, at that time, the method they used to determine DuPont's secrets was considered so out of the ordinary (Fred Wergeles, "Commercial Satellite Imagery: New Opportunities for Competitive Intelligence," *Competitive Intelligence Magazine*). Once high-resolution satellite imagery becomes widely available, it will be harder to argue that overhead observation of the production facilities of rivals is an extraordinary and, therefore, improper means for carrying out competitive intelligence. Instead, businesses may have to take additional steps to protect valuable trade secrets.

Even assuming that the use of satellite imagery for competitive intelligence is considered unlawful, it will be difficult for corporations to prove any wrongdoing by industrial competitors. Current statutes do not require satellite operators to disclose either their imagery or the identity of their clients to third parties. Thus, it is nearly impossible for companies to know whether a passing satellite collected imagery of their facilities and, if so, who asked for specific images. This task becomes even more arduous as the number of domestic and, more importantly, international sources of high-resolution imagery increases. Whereas greater regulation and closer government scrutiny can restrain domestic vendors, controlling international vendors is likely to prove far more elusive.

DRAWBACKS OF COMMERCIAL SATELLITE IMAGING

The widespread availability of commercial high-resolution satellite imagery will for the first time reveal to many people and organizations information to which they never before had access. Some have celebrated this new development, calling it the emerging era of global transparency. But transparency has both positive and negative consequences.

In the field of international relations, greater transparency could allay tensions among international rivals and herald a new era of peaceful coexistence. As one observer stated, "Nations that know what their enemies are doing are less likely to increase world tensions through activities born of fear. And nations that know their enemies are observing them are far less likely to threaten international peace through rash behavior."⁽²¹⁾ According to this view, if everyone is constantly watching everyone else, surprise attacks become impossible and aggressive actions unrewarding.

This premise may often be true, but not always. When the success of aggression is dependent on the element of surprise, transparency will indeed reduce the incidence of aggression. But not all aggression requires surprise to succeed. Transparency could aggravate interstate conflicts by removing ambiguities about relative capabilities and allowing states to exploit each others' weaknesses. To the degree that governments new to remote sensing misinterpret what they see, imagery could create groundless fears.

Even under the best of circumstances, transparency cannot ensure that the right decisions are made. Transparency reveals behavior, but not intent.⁽²²⁾ If enemy troops are detected

massing along the border, is that just harmless posturing, or are they preparing for a preemptive strike? If states reach the wrong conclusions, they may find themselves spiraling uncontrollably toward war.

Transparency could also complicate decision-making by introducing new participants into the policy process. Widespread availability of high-resolution satellite imagery would allow private citizens, nongovernmental organizations, and particularly the media to take a more active role in policy making. These groups could independently use satellite imagery to monitor state compliance with international agreements, expose environmental degradation, and publicize large-scale humanitarian emergencies. In some situations civil society groups and the media might be able to compel states to take action, even when government officials would much prefer to do nothing.

Here again, there are no guarantees that greater transparency will produce better outcomes. Nongovernmental organizations and the media rarely have the resources, analytical skills, or technical expertise that are more readily available to state governments. It is inevitable that organizations will make mistakes as they begin to increasingly rely on satellite imagery. The media have already made such errors on at least four occasions. During the 1986 Chernobyl accident, in an attempt to be the first with breaking news, a number of media organizations misinterpreted imagery and erroneously reported that two nuclear reactors had melted down.⁽²³⁾ Just a few weeks later, a number of networks in the United States cited SPOT imagery of a Soviet nuclear proving grounds at Semipalatinsk as evidence of Moscow's decision to resume nuclear testing. Further analysis revealed that the networks had completely misinterpreted the imagery, falsely presenting routine activities in a far more pernicious light.⁽²⁴⁾

Another error occurred in 1992 when a newspaper called the *European* published SPOT images of what it labeled an Algerian nuclear research complex. Subsequent analysis of the image revealed that the feature in the photo was not a nuclear research facility but a military airbase. To make matters worse, the *European* had published the image upside down and backwards.⁽²⁵⁾

More recently, on May 25, 1998, *Newsweek* magazine published a satellite image that it claimed showed the site in the northern desert state of Rajasthan where India had conducted five nuclear tests. *Newsweek* maintained that the image dated from a week before the tests and ran the picture with several captions identifying specific objects and installations. None of the information was correct. It turned out that the imagery had been collected over five years prior to the blasts, and the feature *Newsweek* identified as the hole where one of India's nuclear explosions took place was in fact an animal holding pen.⁽²⁶⁾

Fortunately, no grave damage has yet resulted from the erroneous reports that have appeared, but it is optimistic to think that continued carelessness will have no consequences. False reporting, whether deliberate or unintentional, could easily embitter relations among nations and prevent the resolution of outstanding disputes.

Transparency raises major economic concerns as well. Radar, multispectral, and especially hyperspectral sensors may allow extraction companies to know more about a country's natural resources than the country's own government. This disparity in knowledge could place state officials at a considerable disadvantage when negotiating drilling rights and mining agreements. As mentioned, governments are not the only ones that may feel an acute

sense of vulnerability. Corporations may find themselves being observed by competitors trying to keep tabs on their construction of new production facilities around the world and estimate the size of their production runs by looking at their emissions.

In short, the emerging global transparency resulting from high-resolution commercial remote sensing satellites promises both benefits and costs. The challenge is to devise policies that harness the benefits of growing international transparency while minimizing its many potential negative consequences.

CONCLUSION

This telephone has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us.

—Western Union internal memo, 1876

Heavier-than-air flying machines are impossible.

—Lord Kelvin, president, Royal Society, 1895

The wireless music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?

—David Sarnoff's associates in response to his urgings for investment in the radio in the 1920s

I think there is a world market for maybe five computers.

—Thomas Watson, chairman, International Business Machines (IBM), 1943

There is no reason anyone would want a computer in their home.

—Ken Olson, president and founder, Digital Equipment Corporation, 1977

640K ought to be enough for anybody.

—Bill Gates, Microsoft Corporation, 1981

The success rate of prognostications about how new technologies will fare approaches zero. No one really knows whether a thriving satellite commercial remote sensing industry will develop over the next decade, or whether the whole industry will crash, figuratively if not literally.

The only sure prediction is that the industry will change, drastically, in the next few years. Some of those changes may come in the form of technological improvements. Space Imaging, operator of the IKONOS satellite now in orbit, recently announced that it is thinking about follow-ons with even greater capabilities. Chief Executive Officer John Cople noted in an interview that the market has changed notably in the four years since the company was formed. Not only is there competition from other potential satellite operators, but “we’re seeing much higher resolution from the aerial companies and would like to be able to participate in that market.”(27) Although there is a widespread myth that Presidential Decision Directive-23 limits the resolution of American satellites to no better than 1 meter, in fact there is no constraint on resolution. Indeed, under ideal conditions IKONOS and some of the other satellites scheduled for launch within the next year will achieve resolutions closer to

0.86 meter. Copple says that the U.S. national security industry, likely to be a major customer, is urging U.S. companies to move to higher resolutions in future satellites.(28)

Some of the changes may involve the organization of the industry. Spot Image of France and OrbImage of the United States recently announced plans for a partnership that would market OrbImage's high-resolution imagery (from OrbView 3 and OrbView 4, planned for launch in late 2000) through Spot's well-established global sales network.(29) Such cross-border alliances are becoming emblematic of the globalization of the industry. Not only are there many countries with civilian or commercial operators, the operators themselves are increasingly multinational enterprises.

If commercial satellite remote sensing does take off, the new availability of imagery will raise further questions for government officials and others around the world, questions not easily answered through purely national means. Because information really is power, the spread of this particularly vivid and comprehensive form of information will ripple through all sorts of relationships—those among states, and those between states and other international actors such as businesses and civil society.

The rapidly growing literature and plethora of conferences on the new satellites have mostly focused on what the availability of high-resolution imagery will do to the conduct of war, and in particular whether it will undermine the overwhelming military preponderance of the United States. Certainly it is possible to imagine circumstances in which the United States would benefit militarily from the suppression of such imagery. It is more difficult to imagine military conflicts involving the United States in which France, India, Israel, Russia, and eventually China would all agree to go along with the suppression of such imagery. This battle is already lost.

The more fundamental questions raised by the new satellites have to do with basic issues about the meaning and relevance of national borders, about the relationships of governments not only to one another but also to private businesses and nongovernmental organizations, and about the meaning of national sovereignty. Satellite imagery is only one of a whole series of information technologies that have caused states to lose control over information about what is happening within their borders. From now on, it will not only be the U.S. Ambassador to the United Nations who can show images of atrocities in the UN Security Council and demand action. Any government on the council will be able to do so, or any government or nongovernmental organization that can persuade a council member to present the images. International negotiations on everything from arms control to climate change, already populated by ever-growing numbers of governments, businesses, and nongovernmental organizations, will face new complications caused by their inability to suppress or ignore unwanted information. Because information will be so widely available, crises may become harder to manage, as leaders find themselves under relentless pressure to act quickly.

But this is not the first time the world has had to adjust to a technologically driven jump in the availability of information. Printing presses were once seen as tools of the devil because they removed control over information from the hands of the medieval Catholic Church and spread it across the (literate) populace at large. Every new step from the telegraph to the Internet has been greeted with proclamations of apocalyptic change. Governments that have tried to suppress and control flows of information have, in the long run, suffered for it. The

wiser course of action, as well as the only practicable one, is to learn to live with the new transparency.

For the United States in particular, it is most unlikely that the shortsighted policy of shutter control will do good, and it could do harm even to the United States itself by undermining an industry on which the national security community will increasingly have to rely. The United States would be better served by policies that return to the traditional U.S. emphasis on open skies and freedom of information. In the 1960s, U.S. policies helped bring about the legitimacy of satellite reconnaissance. In the 1970s and 1980s, U.S. leadership in both the technology and politics of civilian remote sensing led to global acceptance of unconstrained imaging from space. When the inevitable international disputes arise over the new transparency, and when the United States finds itself facing short-term interests in suppressing imagery, it is crucial that it stick to the long-range policies in favor of transparency that have served it so well.

For the rest of the world, this new form of transparency will do far more good than harm. Countries that now live in fear of one another will be able to learn whether those potentially hostile neighbors are in fact mobilizing for attack, and would-be attackers, at least sometimes, will be deterred by the overwhelming likelihood of detection. The pressing environmental and developmental problems facing poor countries, heretofore unseen and therefore easily ignored by the rich, will become both more visible and better understood.

Most important, the new imagery will contribute to a badly needed shift in perspective. As Oliver Morton wrote in an article on satellite imagery in *Wired* magazine in 1997:

Like the telephone or the wrist watch, it is the sort of product that gets woven into the fabric of life—in this case, as an assumption that all the world is out there to be seen, that it is all available, comprehensible, and held in common.... With shared eyes we will watch the world carry its cargo of civilization—its roads, its fields, its cities, its landfills—through time and space. This portrait will be an image that can zoom in to the personal and pull out to the geopolitical, a new way to look at borders, a new way to look at news. It will be an illustration of everything: not, in the end, a view from nowhere, but a view from everywhere, for everyone.(30)

NOTES:

1. For the Real Video, transcripts, and summary of different presentations at the conference, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/Agenda.htm.
2. Ralph Rugoff, "Fame," *LA Weekly*, July 30, 1999.
3. For a discussion of the security implications of commercial high-resolution satellites, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/BakerPage.htm; www.ceip.org/programs/transparency/RemoteSensingConf/BernsteinPage.htm; and www.ceip.org/programs/transparency/RemoteSensingConf/MullenPage.htm.
4. Peter D. Zimmerman, "The Uses of SPOT for Intelligence Collection: A Quantitative Assessment," in Michael Krepon, Peter D. Zimmerman, Leonard S. Spector, and Mary Umberger, eds., *Commercial Observation Satellites and International Security* (Washington, D.C.: Carnegie Endowment for International Peace, 1990), p. 77.
5. It is well documented that during the Iran-Iraq war, images of battle areas were purchased frequently. It is not clear, however, who acquired the imagery or for what purposes. See Peter D. Zimmerman, "From the SPOT Files: Evidence of Spying," *Bulletin of the Atomic Scientists*, Vol. 45, No. 7 (September 1989), p. 24. Further, it has been reported that "before invading Kuwait, Saddam Hussein bought imagery from the French SPOT

- satellites,” although the information could not be corroborated by the authors. See also Robert Wright, “Private Eyes,” *New York Times Magazine*, September 5, 1999.
6. Report 102-539, U.S. House of Representatives, Committee on Science, Space, and Technology, May 28, 1992, p. 26.
 7. This level of detail is possible only if the sensor has a high enough spatial resolution and can detect objects in the long-wave segment of the spectrum.
 8. For more details visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/PikePageHumanitarian.htm.
 9. David Rohde, “A High-Tech Threat with a Low-Tech Track Record,” *New York Times*, April 4, 1999, p. 6.
 10. The groups included: Physicians for Human Rights, Refugees International, International Crisis Group, Network Bosnia, Coalition for International Justice, Institute for the Study of Genocide, Freedom House, Network of East-West Women, Balkan Action Council, and Minnesota Advocates for Human Rights. Nora Boustany, “The Heavens Look Down on Kosovo,” *The Washington Post*, April 2, 1999, p. A19.
 11. For more details, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/HammondPage.htm and www.ceip.org/programs/transparency/RemoteSensingConf/JanetosPage.htm.
 12. The retreating Iraqi troops set between 640 and 650 oil wells alight; some, however, were already extinguished by the time Landsat imagery of the oil fields was collected. Peter D. Zimmerman, “The Use of Civil Remote Sensing Satellites During and After the 1990-91 Gulf War,” *Verification Report*, VERTIC (1992), p. 239.
 13. Frederick P. Hafetz and Gwen M. Schoenfeld, “Advanced Measurement Techniques: Technological Breakthroughs May Usher in Era of Change,” *Environmental Compliance & Litigation Strategy*, Vol. 13, No. 3 (August 1997), p. 1.
 14. Karen Litfin, “Public Eyes: Satellite Imagery, the Globalization of Transparency, and New Networks of Surveillance,” unpublished manuscript, 1999.
 15. For more details on the media uses of satellite imagery, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/DubnoPage.htm and www.ceip.org/programs/transparency/RemoteSensingConf/LivingstonPage.htm.
 16. Oliver Morton, “Private Spy,” *Wired* (August 1997), p. 1.
 17. *Ibid.*, pp. 9-10.
 18. Pierre C. Robert, “Remote Sensing: A Potentially Powerful Technique for Precision Agriculture,” paper presented at the conference titled Land Satellite Information in the Next Decade II: Sources and Applications, American Society for Photogrammetry and Remote Sensing, Washington, D.C., 1997.
 19. “Offshore Oil Detection: Radar Imagery Offers a Slick for Locating Rich Reserves at Sea,” *Imaging Notes*, Vol. 14, No. 2 (March/April 1999), p. 24.
 20. Fred Wergeles, “Commercial Satellite Imagery: New Opportunities for Competitive Intelligence,” *Competitive Intelligence Magazine*, Vol. 1, No. 1 (April/June 1998), p. 37.
 21. R. Jeffrey Smith, “High-Tech Vigilance,” *Science* (December 1985), pp. 26-33.
 22. Ann M. Florini, “The End of Secrecy,” *Foreign Policy*, No. 11 (Summer 1998), p. 60.
 23. Dino A. Brugioni, “Satellite Images on TV: The Camera Can Lie,” *The Washington Post*, December 14, 1986, p. H1.
 24. *Ibid.*
 25. Vipin Gupta, statement made during the Carnegie Endowment for International Peace conference entitled No More Secrets: Policy Implications of Commercial Remote Sensing Satellite, Washington, D.C., May 26, 1999. To watch the Real Video of Vipin Gupta’s presentation, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/GuptaPage.htm.
 26. Statement made by Steven Livingston at the Carnegie Endowment for International Peace conference entitled No More Secrets: Policy Implications of Commercial Remote Sensing Satellites, Washington, D.C., May 26, 1999. See also “Correction” in the August 31, 1998 issue of *Newsweek*. To see more of Steven Livingston’s presentation, visit the Carnegie Endowment for International Peace website at www.ceip.org/programs/transparency/RemoteSensingConf/LivingstonPage.htm.
 27. Warren Ferster, “After IKONOS, Space Imaging Plans Even Better Satellite,” *Space News*, Vol. 10, No. 36 (September 27, 1999), p. 3.
 28. *Ibid.*
 29. Warren Ferster and Peter B. de Selding, “Spot Image, Orbital Plan Reciprocal Sales Deal,” *Space News*, Vol. 10, No. 36 (September 27, 1999), p. 3.
 30. Oliver Morton, “Private Spy,” *Wired* (August 1997), p. 9. FINALreport.qxd 2/17/00 6:54 PM Page 37

INTERNATIONAL VIEWS OF OSINT

TEACHING THE GIANT TO DANCE: CONTRADICTIONS AND OPPORTUNITIES IN OPEN SOURCE WITHIN THE INTELLIGENCE COMMUNITY

Admiral William Studeman

FAS Intro: The following discussion of the history of the Foreign Broadcast Information Service and open source intelligence was presented by Admiral William Studeman at the First International Symposium on Open Source Solutions in December 1992. It is reproduced here with the permission of Open Source Solutions, Inc.

It's a pleasure to be here today to take part in this symposium. This is truly an exciting time -- a revolutionary time -- to be in the intelligence business. And no area is full of more promise for intelligence than open source access and exploitation. In my only reference to dancing, you can consider this presentation as an attempt to describe how we move the Intelligence Community giant from the square dancing era of yesterday to the open source Lambada of tomorrow.

A number of people that I've talked to -- including Members of Congress, journalists, and the public -- have asked me to explain why intelligence organizations are interested in unclassified information. So I'd like to begin by asking a rhetorical question: "why does the Intelligence Community collect and analyze open source data?"

This is not a new issue for intelligence. As you know, intelligence has drawn broadly on open sources for many years. FBIS -- the Foreign Broadcast Information Service -- has collected, analyzed and reported open source intelligence from all over the globe for over half a century -- and it has done a superb and highly valued job.

The information that FBIS has collected over the years has been critical to US national security decision makers.

- Few people realize that during the 1962 Cuban missile Crisis, through monitoring Radio Moscow, FBIS provided President Kennedy with the first news of the Soviet decision to withdraw missiles from Cuba.
- At times, public information has been the Community's only source during a crisis. For example, during the 1956 Hungarian uprising and the 1968 invasion of Czechoslovakia, radio broadcasts provided intelligence analysts with highly relevant, timely understanding of what was happening in the streets of Budapest and Prague.
- Open sources can also provide tip-off or early warning of events. You may be interested to know that the change in policy leading to the February 1989 Soviet military withdrawal from Afghanistan was identified in FBIS media analysis reports as early as May 1985.
- More recently, CIA analysts who monitored the collapse of the Soviet Union estimate that at least 80% of their information came from open sources.

- And now, intelligence analysts are using open sources to monitor the Yugoslav crisis. They study transcripts of radio broadcasts by both sides to gain insights into the intensity of the conflict and the probable outcome.

Although all of the intelligence Community has relied on open sources for many years, some people who are not familiar with our business are confused about how intelligence uses information that is available to the public.

The first thing that people must understand is that intelligence is not competing with the media. But intelligence and the media are in the same business; that is, ultimately, to tell a story of relevant interest, but in our case, the story normally relates to a threat or a foreign issue of high or potential interest to U.S. or allied policymakers, planners, or warfighters. Our goal is not necessarily to produce raw open source data, but to glean information from open sources that is of interest to intelligence *as background* reference material for collectors and analysts/producers, and, more importantly as a source of information to be fused with data from classified sources and methods and this is again principally for the government customer.

Our analysts rely on a multiplicity of sources -- including signals, imagery, human and other classified intelligence sources as well as openly available data -- to produce their reports.

Foreign intelligence and counterintelligence earns its money first by maximizing these *classified* sources and methods, and secondly by building highly structured analysis and production systems which are highly responsive to the widest range of U.S. and allied customers, be the topic political, military, economic, environmental, sociological, law enforcement support, or otherwise.

But good intelligence officers, like media personnel, are essentially information hounds. The highest emphasis is placed on timeliness, relevancy, accuracy, and completeness of data disseminated at the lowest and most readily usable classification level and tailored to the diverse sets of simultaneous users at varying echelons of the bureaucratic structure from the President to lowest platoon leader and beyond.

The highest form of intelligence enlightenment is the dynamic and continuous fusion of data from all available sources. In this blending process a great synergy results, and this magic cannot be accomplished without unconstrained and continuous access to open source data. Open source can provide event specifics, background context, focus, contrast, improved accuracy, alarms, and many other positive features associated with data manipulation in an information age.

While untrustworthy data can often be associated with classified sources and methods, open source data can be a frequent source of biased and misleading information, or worse yet, the product of deliberate deception or information control practiced in parts of the world by a less free press that may also operate as a propaganda instrument of government forces. This dictates that a strong data evaluation system be in place for use with open source data, as it is for classified data.

On the positive side, when an open source contradicts other intelligence sources -- or other open source reporting -- it serves as a flag for the analyst to re-evaluate his or her analysis. For example, at a time when there was wide intelligence speculation that the Dominican

Republic might extradite a terrorist, an FBIS report called attention to a press account that the Dominican president had said he would not extradite the terrorist.

Utilizing intelligence analysis techniques, it is frequently possible to interpret or predict events based on open source usage. The evidence is often acquired through laborious textual analysis -- and by comparing media content with past actions.

- For example, FBIS analysts anticipated the February 1979 Chinese invasion of Vietnam by demonstrating that, with rare exceptions, the wording of authoritative Chinese warnings to Vietnam had only been used in instances in which Beijing had actually applied military force.

On some occasions, intelligence analysts adjudge open source information to be more accurate than classified sources. This can derive from either the weight and credibility of open sources versus the untested, contradictory or poor performing nature of the classified sources or from some other evaluation criteria. When we do favor unclassified sources over classified sources, we need to be sensitive to the credibility we have lent the data by adopting it as our own position.

Most people in our business agree that open sources have proven to be enormously invaluable to intelligence. Even during the Cold War, when intelligence was focused principally on acquiring secret information, open sources gave us some highly usable glimpses into closed societies. Today, with a generally more open world and a considerably more free and independent world press, open sources have even greater value for intelligence. In the new global environment, open sources provide much more hard, credible data about a wide range of international political, social, and economic issues.

There is a complex relationship between the way open source material is mixed with classified data and the concept of openness. We frequently have products where only a small amount of the overall data comes from classified sources requiring security protection. We have security procedures in effect to clearly mark paragraphs which possess classified data, and this enables much greater sanitization of intelligence publications to the unclassified level. The more complete and expansive the open sources, the more likely we can produce a wider variety of unclassified or lower classification products using the classified data as background for confidence-building and credibility. It is important to recognize that once an Intelligence Community agency puts its name on an essentially unclassified product, it may assume an enhanced credibility beyond that of the original open sources. This obligates the Intelligence Community to high standards of quality control, which we would expect of our people, in any case.

The Intelligence Community's current challenge is to expand the use of open sources to cover a broader range of issues -- such as weapons proliferation, economic competitiveness, and the environment. As one example, it is estimated that some 80% of the information needs for environmental intelligence can be met through information that is available to the public.

As you are well aware, the quality and quantity of open source information continues to grow:

- We have identified some 8,000 commercial data bases -- and the vast majority have potential intelligence value.

- The number of worldwide periodicals has grown from 70,000 in 1972 to 116,000 last year.
- The explosion of open source information is most apparent in the Commonwealth of Independent States, where today, there are some 1,700 newspapers that were not published three years ago.
- While the number of TV and radio stations around the world has not experienced rapid growth, the broadcast time and breadth and depth of their coverage, and the availability of cable TV are clearly on the upswing.
- The sources of "grey literature," (i.e., private or public symposia proceedings, and academic studies) around the world are also increasing dramatically.

As you know, open source encompasses a wide array of mediums -- including printed material, such as books, magazines and newspapers; as well as maps, photographs, data files, digital imagery and broadcast media -- both radio and television. These multimedia open source inputs correspond well to the range of product *outputs* used by the Intelligence Community. These intelligence outputs tend to be multimedia in nature, including hard copy and electronic dissemination of written and formatted, man and machine readable text, imagery, graphics, maps, and other situational displays as well as video. Because of the need to move data quickly in worst case situations, electronic information handling and display systems are most common. Most of these intelligence systems use off the shelf hardware, open systems, commercial architecture and operate as part of large area networks. The Intelligence Community has a special problem managing multilevel security in systems where open source data is mixed with classified data.

I'd like to say a special word about TV -- because it is a relatively new area for intelligence. Each week, FBIS monitors 790 hours of television from over 50 countries in 29 languages. Foreign TV programs -- such as news programs and documentaries -- give analysts a multidimensional feel for a country or material that other open source media cannot provide. Many analysts prefer to see the way a particular country chooses to portray events visually, rather than relying on the news network "filter." Coverage of foreign television brings us closer to what is happening in all areas of the world; it allows us to monitor crises as well as to broaden our knowledge of more restrictive societies. For example, the revolutions in Eastern Europe were covered extensively on those countries' domestic television.

In addition to analyzing foreign television, intelligence organizations are producing classified videos for policy makers which incorporate information from foreign news programs. The end result is a high-impact intelligence product used exclusively in the government that improves policymakers' understanding of complex issues.

The dramatic increase in open source material, its wide variety -- and its increasing value to intelligence -- demand a revolutionary change in the intelligence Community's approach to open source management, collection, processing and dissemination.

Unlike the other collection disciplines, which are highly structured, open source is not a tightly integrated discipline in the Intelligence Community. Over the years, open source information collectors, processors, and users have been diverse and decentralized groups spread across the breadth and depth of the Community. As a consequence, the various agencies in the Community didn't know the extent of unclassified holdings of other agencies, and had virtually no capability to share electronically the information which they did possess.

In short, the Community lacked a unifying structure, and a coherent and consistent set of overall requirements for the collection, processing, exploitation, and dissemination of open source information.

A DCI Task Force was formed last year to make recommendations on these issues -- and important changes are underway. As a result of the task force, for the first time the DCI has established an Open Source Coordinator (Paul Wallner of the Defense intelligence Agency) who is:

- cataloging the open source holdings of the Community as a whole;
- establishing a comprehensive requirements system for the Community; and
- establishing interconnectivity so open source information can be shared throughout the Community.

Another responsibility of the Open Source Coordinator is to interact with the managers of the other collection disciplines to ensure that they are not collecting against requirements that can be satisfied through open source materials.

In my view -- and this is a view shared by many throughout the Community -- open sources should be the Community's first step in a range of choices to meet our overall information needs. Compared to information collected from satellite and other reconnaissance and surveillance means, open sources are relatively inexpensive to acquire. It would be both bad acquisition management and information management to waste a costly intelligence asset collecting information that can be acquired through an open source.

Although I believe that open source should be the Community's first step in attempting to satisfy our information needs, I want to emphasize that it will likely never replace the other intelligence collection disciplines. But I do strongly believe that better and complementary management of open source assets will, in turn, lead to more efficient and focused use of those other collection disciplines.

Without question, the biggest challenge the Intelligence Community faces with respect to open source is processing the vast amount of data available.

Intelligence organizations have significant expertise processing and filtering large quantities of data, putting it on mass storage, manipulating it (including translation or gisting), and devising systems to have data available to analysts on an on-call basis.

In fact, US intelligence operates what is probably the largest information processing environment in the world. Consider this: Just one intelligence collection system alone can generate a million inputs *per half hour*; filters throw away all but 6500 inputs; only 1,000 inputs meet forwarding criteria; 10 inputs are normally selected by analysts and only one report is produced. These are routine statistics for a number of intelligence collection and analysis systems which collect to technical intelligence.

In the open source arena, FBIS monitors over 3,500 publications in 55 foreign languages. And each day it collects a half a million words from its field offices around the world and another half a million words from independent contractors in the US -- that's equivalent to processing several copies of *War and Peace* every day.

These two examples show the magnitude of the classified data and translation problems facing an already data-rich Intelligence Community. The open source challenge can theoretically present ever more daunting levels of data and translation requirements, reaffirming that information management will be the single most important problem for the Intelligence Community to address for the future.

In this equation, one of the dilemmas posed deals with how we will spread our already overtaxed Intelligence Community information management resources in the context of both people and systems across both the classified and open source collection and analysis areas. This conference can hopefully provide some pointers to solutions in this area, mindful of the fact that we are in a period of intelligence budget austerity and Community downsizing.

Of course, the key issue for intelligence analysts is not simply the quantity of open source data that is collected, but also its quality -- that is, its intelligence value.

Open source information is produced or published largely according to the needs of the private sector, without regard to the uses to which that information will be put by the intelligence customers.

At the present time, open source materials that are collected for intelligence are often not made available to analysts in a way that is useful to them. And there is only limited ability to search large open source holdings in a timely manner.

A substantial amount of open source information is reported in foreign languages and require translation. For example, in FY '92, FBIS translated 200 million words-- so the translation issue is another dimension to the information management challenge.

Much of the Intelligence Community's current open source architecture was developed in an age when information processing and communication were in their infancy. As we look to the future, we will have to develop more creative approaches to manage the vast amount of data being produced.

Based on the recommendation of the DCI Task Force, the Community-wide Open Source Steering Council has developed a Strategic Plan that presents a vision of the intelligence Community's goals for open source collection ten years from now.

The plan establishes the goal of creating an integrated Community open source architecture. The new architecture must provide, among other things:

- flexible collection,
- networked access to external data bases,
- immediate user and customer feedback, and
- automated, profiled delivery of collected open source information based on user requirements.

We expect the centerpiece of the architecture will be an Open Source Information Exchange - - comprising a central switch and digital communications networks which interconnect all user organizations within the Community.

The inputs to the Open Source Information Exchange will be government sources, such as the Library of Congress; the FBIS electronic dissemination system; and the vast array of commercial sources, such as NEXIS.

The system will distribute open source data through "functional support centers" that are being developed and funded by the Community. These functional support centers will serve as focal points of expertise on critical intelligence topics -- such as science and technology; and political, military, and economic intelligence.

The strategic plan begins with a vision for timely access to open source data, and identifies funding, management, and architecture considerations. It also establishes strategies and out-year timetables for open Source Coordinator pursuit of a more integrated open source design and implementation effort to support the widest variety of Community analysts and policymakers. Finally, it deals with specific requirements, collection, processing, exploitation, dissemination-related goals and objectives in specific detail. The plan is ultimately a roadmap for Intelligence Community-wide transition from the current way of doing business to future mode of operation. Its principal features bring us:

- from partial connectivity to full interconnectivity;
- from reliance on hard copy to digital electronic data;
- from dependence on physical information centers to the establishment of electronically-connected, virtual information exchanges;
- from querying one data source at a time to querying many at once;
- from the use of multiple standards and tools to common standards and tools;
- from development of sophisticated data bases on only a few topics to the creation of a wide range of data bases on many subjects;
- from limited access by users to sources of data to broad, flexible access;
- from emphasis on the collection and dissemination of data to a balance between that and making data readily accessible and tailored to user and customer needs;
- from a limited ability to display data to the ultimate application of fast developing multimedia capabilities.

Many important questions must be considered along the way. Open source is being considered by the DCI as the equivalent of a dominant intelligence discipline. In the restructuring of national intelligence, we have structural agency czars who are focused on and accountable for the management of national disciplines; for example, NSA for SIGINT, CIO for Imagery and the CIA/DO for HUMINT. Open source is far more decentralized in its current and even its envisional approach and management. *Will* the time come when we need more focus and accountability in open source management, mandating the establishment of a structural czar for this critical area?

How will we change the mindset of those people in the Community who do not yet think of open source as a bona fide collection discipline on a par with SIGINT or IMINT, or HUMINT?

There is no question that open source -- in comparison with other collection systems -- has the potential to provide a lower cost, lower risk supplement to intelligence collection and analysis. But access to open source data still costs money. So another question the Community will have to consider is, "Just how much money will be available to spend on managing open source data in an era of potentially *dramatically* declining resources?"

An expanded use of open source material raises legal questions -- especially concerning licensing agreements and copyright protection. Lawyers and managers in the Intelligence Community are working diligently to ensure that our use of copyrighted information strikes the appropriate balance between the government's legitimate need for access to open source material with the copyright owners rights and privileges.

For instance, the Intelligence Community, like any other commercial user, buys access to a number of commercial data bases. When one component of the Community is licensed to use a data base, can it disseminate that data, or provide access to other users in the Community? If the answer is not clear, we work with our commercial vendors to revise our basic agreement to ensure that our use of the material is consistent with our agreements with the vendor.

I would like to conclude by reminding you that the great strength of American intelligence, which is unique in the world, is its ability to responsibly manage a global intelligence system, continuously moving bits of data from diverse sources to a broad and demanding customer-set. That new customer-set has even more highly distributed information requirements for the future.

Fundamentally, it is the hundreds of messages and other intelligence products that we electronically disseminate hourly which constitute the bread and butter of the intelligence business. Our implicit requirement is to manage a virtual intelligence system which adapts its multimedia products to the demanding users in a changing and unsettled world environment. Open source material fits legitimately and prominently into the equation of modern intelligence sources and methods, but presents special challenges and dilemmas for us to resolve.

Well, that's a lot to think about -- and I can assure you that the Intelligence Community is well aware of the opportunities -- and the challenges -- associated with open source in our world today and of tomorrow. And we plan to draw on the expertise of the private sector, other government agencies, and the academic community to meet these challenges in the years ahead.

This conference is just one way we can help to make all this happen. Thank you for your interest in this important topic; we look forward to continuing to work with you in the future as we attempt to address these and other problems associated with the provision of focused intelligence and information support to our customers in a changed and changing world. Thank you for the opportunity to be with you today, and I wish you well for the remainder of this timely and important conference.

OPEN SOURCE INTELLIGENCE: WHAT IS IT? WHY IS IT IMPORTANT TO THE MILITARY?

Robert D. Steele, President OPEN SOURCE SOLUTIONS, Inc.

<http://www.oss.net/>

Introduction

This White Paper defines Open Source Intelligence (OSCINT) and its relevance in meeting the needs of the military (both commanders and defense policy-makers).

OSCINT is intelligence derived from public information--tailored intelligence which is based on information which can be obtained legally and ethically from public sources.

This White Paper suggests that OSCINT is a both force multiplier and a resource multiplier. OSCINT provides a practical political and military advantage which complements the advantage provided by traditional intelligence, it is available at low cost, and it cannot be ignored.

First the paper describes and discusses the utility of OSCINT in general terms, and at the strategic, operational, tactical and technical levels of warfare, including a single practical example at each level. The paper then describes the "information continuum" within which a range of open sources, systems, and services can be obtained which are relevant to military needs. Finally, the paper provides a brief discussion of the status of the open source intelligence programs in the United States, The Netherlands, and Sweden, and concludes with a concise discussion of opportunities and risks inherent in the use of OSCINT to meet military requirements, and of several practical steps that can be taken to exploit OSCINT in support of military strategy, operations, tactics, and technical acquisition and countermeasures.

The official definition of OSCINT by the U.S. Intelligence Community:

By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROM's. It may be disseminated to a broad public, as are the mass media, or to a more select audience, such as grey literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with U.S. or foreign persons; or is acquired through clandestine or covert means.

The official definition is limited in its understanding to standard commercial sources of traditional information, and excludes, to take one important example, SPOT imagery. It also fails to take into account the importance of unpublished materials including electronic information and human knowledge which can be accessed legally and ethically.

The official approach to OSCINT is also limited in that the existing information-handling architectures for intelligence processing, including dissemination to the commander, are all classified, and there is a very limited capability for routing unclassified information efficiently, even assuming it can be obtained. In most communities, there appears to be a

reluctance to assume primary responsibility for the collection and processing of OSCINT, which is why military operators in two countries (the United States and the United Kingdom) are examining means of acquiring and exploiting OSCINT directly, bypassing the intelligence community in order to give action officers at the policy level, and commanders at the operational level, direct access to OSCINT.

Experienced intelligence professionals have found that while OSCINT is not a substitute for traditional intelligence disciplines, including Human Intelligence, Imagery Intelligence, and Signals Intelligence. However, OSCINT does offer three major advantages for planning and conducting military operations:

- When encountering requirements for military operations in the Third World or in support of humanitarian assistance and counter-terrorist operations for which intelligence collection priorities have not been high, OSCINT is frequently the only discipline able to respond rapidly (to include commercial imagery), and it provides the commander and his staff with a rapid orientation adequate for both developing initial planning packages; and for establishing collection requirements for the traditional intelligence disciplines.
- OSCINT is also a means of achieving significant savings, in that many essential elements of information required by the commander and his staff can be acquired from commercial sources at a lower cost, in less time, than from classified capabilities, with the added advantages that OSCINT is often more up to date, and requires no political risk in its acquisition. This permits classified intelligence capabilities to be focused quickly and effectively on mission-critical gaps, and avoids depleting or misdirecting these scarce resources-- "do not send a spy where a schoolboy can go".
- Finally, OSCINT, whether it precedes or follows traditional intelligence collection, can protect national intelligence sources and methods by serving as the foundation for intelligence support to joint and coalition operations where it is not possible, or desirable, to reveal the capabilities and limitations of the traditional intelligence community.

Open Source Intelligence and the Military

The availability and utility of OSCINT depends upon, and will vary, depending on the specific area of operations under consideration, and on two other factors: the level of warfare, and the point on the spectrum of conflict, from presence to general war, where the intelligence will be applied.

In general terms, OSCINT has significant potential as a source of intelligence support in terms of indications & warning, policy development, contingency planning, security assistance, weapon acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting the commander and serving as the foundation for collection management within the traditional intelligence disciplines.

At the strategic level:

- OSCINT can provide indications & warning of both hostile intent, and opportunities for military advantage. Content analysis of multiple open sources such as regional newspapers from the Middle East, are often if not always more reliable foundations for estimating stability and instability, than reports from clandestine sources with a limited range of access and a personal perspective that biases their reporting.² OSCINT is especially valuable with respect to cultural and demographic intelligence, areas not generally well- covered by traditional civilian and military intelligence collection and analysis capabilities.
- OSCINT can also provide very important geographic and civil generalizations which can significantly affect major military acquisition and design decisions. For instance, most countries build their aircraft for optimal performance on a "standard aviation day" which is defined in terms of warm (60-70 degrees) conditions and balanced humidity. The military commander that is responsible for expeditionary operations to the Third World will find themselves utilizing aircraft which carry half as much half as far because the standard aviation day in the Third World is hot (over 80° with high humidity). If aircraft cannot be designed for optimal performance on a hot day, then the military commander can at least ensure that doctrinal publications reflect accurate load and lift capabilities for the true expeditionary conditions to be encountered.
- OSCINT can provide unclassified threat intelligence which can be used to educate and mobilize public and political support for military needs including policy development.

At the operational level:

- OSCINT can provide the geographic and civil generalizations required for regional force planning and force employment. In particular, OSCINT has established credible regional generalization regarding the capabilities of air, ground, and sea forces to be encountered by the commander; geographic generalizations with respect to cross-country mobility, average line of sight distances, temperatures, and water availability; and civil generalizations such as bridge-loading, port clearance, airhead bunkering; and civil communications and computing resources. OSCINT provides a time-sensitive solution to questions the theater commander will have about civil infrastructure, political cliques and personalities, and economic or financial factors affecting operational employment of forces, and is therefore especially helpful to contingency planning which must be pursued without adequate support from traditional intelligence capabilities.
- OSCINT is especially useful to the theater commander for the coordination of joint and coalition operations where traditional classified intelligence capabilities are either not available (e.g. in much of the Third World where lower priorities have restricted coverage), or cannot be shared with foreign elements.

At the tactical level:

- OSCINT has been shown to be highly pertinent and effective against new priorities, including counter-proliferation, counter terrorism, and peacekeeping operations. This

is true for both conventional military operations focused on overt interdiction, and clandestine or covert "direct action" by special operations forces.³

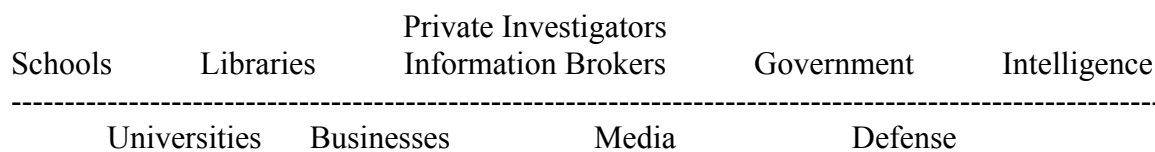
- OSCINT is a critical resource for the military commander who requires maps and digital targeting information for Third World area for which current geographic information is not available from government sources, whether classified or unclassified. In combination, SPOT and other commercial imagery resources can provide the commander with up to date maps containing all airfields, roads, and bridges; and soon containing contour lines as well, for expeditionary operations.⁴

At the technical level:

- OSCINT about civil communications and computing capabilities in the area of operations will be very important to the commander. As information warfare and information peacekeeping become critical mission areas, and all opponents achieve some capabilities to conduct electronic warfare, the commander will need to use OSCINT both to understand how to degrade the performance of civil capabilities being used by opponents, and to consider exploitation of civil capabilities to maintain joint and coalition communications.
- OSCINT will provide most of what the commander needs to plan and coordinate joint and combined air, sea, and land operations in the expeditionary environment, with specific reference to strategic airlift and sealift operations involving civil aircraft, air traffic control and air defense planning for civil platforms, and fueling and other logistical considerations.

The Information Continuum

There are three ways of understanding the robust nature of the private sector's potential contribution to military intelligence needs. The first is by examining in general terms this continuum.



Each of these nine sectors of the global or national information community maintains a cadre of human experts as well as a range of both hard-copy and electronic information. Much of what is known to them, or stored by them, is not available through commercial online services. Following a specific example from each sector:

- Language schools can rapidly identify individuals by location and nationality who have received training in the home country language and are target country nationals (e.g. Somalis studying French in Paris); these individuals can be contacted and offered part-time employment as translators.
- Universities utilize their existing infrastructures and a regular supply of cheap intellectual labor to maintain important and authoritative databases. The Monterey Institute of International Studies, for instance, maintains the best database on the

proliferation of nuclear materials, and utilizes graduate students fluent in Russian, Chinese, Arabic, and other languages to cover a wide range of multi-lingual publications, and to maintain an electronic database, at very low cost.

- Libraries can be used, either as needed or in a deliberate fashion, to serve as repositories for "just in case" archiving of political-military, economic, and other materials pertaining to specific countries. This allows the government to share the cost of archiving with other library sponsors, and in many cases avoid the cost altogether.
- Businesses have enormous repositories of market research, including communications and logistics research, on countries throughout the world where they have made or plan to make an investment. Businesses are also acutely familiar with the political corruption, climate conditions, and other factors which affect operational efficiency in specific locations. Two unique examples of business dedicated to meeting private intelligence needs are Oxford Analytica, with its network of 750 overt agents worldwide, and The Economist Intelligence Unit.
- Information brokers can be identified who specialize in particular scientific & technical topics or regions of the world. This permits more efficient search & retrieval by exploiting capabilities whose "learning curve" has been funded by others. In addition, information brokers can be identified with specific language capabilities, and employed to do rapid exploitation of captured or acquired documents.
- Journalists responsible for specific areas of the world, including journalists specializing in military, aerospace, and insurgency matters, rarely publish ten per cent of what they know, and they never publish their sources. They can, however, be engaged to prepare special reports, and to provide background information on specific personalities of importance to planned military operations. This need not be done secretly or through direct recruitment; it can be done discreetly as a private commercial transaction. Media organizations, such as Jane's Information Group, acknowledge that they publish less than 20% of what they know, in some cases to protect sources--they are however willing to do tailored confidential reports drawing on their complete range of sources.
- Governments, including provincial and state governments, frequently have experts in agriculture or other trade-related fields who are familiar with specific areas of operation and the logistics as well as the key personalities. Embassies have personnel whose reporting does not fully communicate what they know. Bringing key government personnel together for a week can quickly establish a foundation for collection management which the commander could not normally achieve through analysis of raw information.
- Other intelligence organizations, including the "information and research" elements of the Vatican, the United Nations, and the International Red Cross, have global networks of reporting sources, including sources with special linguistic and regional skill, that can be drawn upon.

The third way of understanding the robust capability of the private sector is to consider the range of information services that are offered which are directly pertinent to military intelligence needs. These are listed in three columns:

Direct Observation	Document Acquisition	Telephone Surveys
Commercial Online Searching	Document Translation	Market Research
Current Awareness	Broadcast Translation	Recruited Agents
Experts On Demand	Multi-Expert Research	Industrial Espionage

Recruited agents and industrial espionage are not considered legal nor ethical within the private sector, but there are very competent organizations that openly offer such services, to include route reconnaissance and target identification services in third countries. In each of the above categories, it is highly likely that a private sector partner can collect, process, translate, and deliver open sources of intelligence able to make an important contribution to the commander's needs for information--and to do so in a cost-effective fashion which could not be duplicated by defense attaches or traditional military intelligence collection brigades.

The third way to understand the utility of the private sector for military intelligence needs is to take a case study, such as Somalia. In the absence of internally-available intelligence information, the fastest means of establishing an encyclopedic foundation for further collection management, and the fastest means of providing the commander with at least some useful information pending responses from the traditional intelligence disciplines, it by seeking out private sector experts and private sector databases. A leading scholar, a leading businessman recently returned from a tour as General Manager in Somalia, a leading journalist, and perhaps an information broker specializing in African information could be brought together and could quickly identify human, hard-copy, and electronic sources--including sources of digital geographic information--of immediate utility.

In one specific instance, supporting a wargame on Somalia, an individual playing the role of the United Nations commander was able to overcome the inadequacies of the U.S. intelligence community by making three telephone calls. Overnight, in Express Mail, at a pro forma cost of about \$5,000, the individual received:

- From Jane's Information Group, a spiral-bound volume containing a map of Somalia clearly marking the nine clan areas; a one-page order of battle for each clan (at a time when most intelligence analysts were thanking only of the old Somali army); and a one- paragraph précis with full citation for each article about Somalia published in any of the Jane's publications (including the excellent Jane '5 Intelligence Review) in the past two years. This constituted a superb orientation for both planning and collection management.
- From Oxford Analytica, twenty two page reports suitable for Presidents and Prime Ministers, covering three topical areas: United Nations operations in Somalia, U.S.

foreign policy toward Somalia; and U.S. operations related to Somalia. Again, a superb orientation on strategy and policy, in concise and immediately-usable form.

- From The Economist Intelligence Unit, a copy of the appropriate country risk report, which included important summary information on the logistics difficulties that would be encountered, including the limitations of both the port and the airfields for strategic entry.

Commentary on Representative National Approaches to OSCINT

Although OSCINT has always been part of the national and military intelligence process, in recent decades increased emphasis on technical systems and secret collection have tended to sharply reduce the amount of funding and the number of personnel dedicated to collecting and processing publicly available information. At the same time, the "information explosion" or "information revolution" has dramatically increased both the quality and quantity of the information available in the public sector. Today the commander can take a weather map of Bosnia off of the internet, or exchange email with volunteer observation and listening posts in Bosnia.

Unfortunately, the reality today is that most intelligence communities are trained, equipped, and organized to collect and process secrets. OSCINT capabilities in both the civilian and military sectors of government have both atrophied where they existed, and also failed to keep up with the growth of private sector OSCINT capabilities.

- United States of America. The National Foreign intelligence Board was recently briefed to the effect that while 99% of the \$28-35 billion dollars a year budget is spent on classified collection and processing, and only 1 % is spent on OSCINT, OSCINT provides 40% of the all-source product. in one interview, the Deputy Director for Science & Technology of the Central Intelligence Agency stated that this latter figure was actually 70%. The major element of the U.S. intelligence community program is the Foreign Broadcast Information Service, which is under severe criticism for its continued emphasis on print media exploitation, and its inability to master a wider range of open sources. in an attempt to gain control over the modest distributed resources being applied to OSCINT, the Director of Central intelligence created the Community Open Source Program Office. This office is about to release a strategic plan for OSCINT, but it is limited to improving internal community access to open sources already collected. The Department of Defense program, for which the National Air Intelligence Center is the executive agent, builds on the existing scientific & technical intelligence document acquisition and translation program. The Department of Energy laboratories, and especially Sandia and Los Alamos, constitute a major OSCINT resource which is being exploited by some military consumers of intelligence, such as the U.S. Southern Command, but which is not under the control of the intelligence community. Some very modest individual initiatives have taken place within the military services, the most advanced of which is the publication, in draft form by the Army, of an open source primer for military intelligence officers. At this time the U.S. military does not have timely broad access to a full range of open sources.⁵
- The Netherlands. Various open sources, including the Intelligence Newsletter out of Paris, and OSS NOTICES in the United States, have reported that the foreign and

military intelligence agencies have been integrated. Within the new national intelligence agency, a special Open Source Coordinator has been appointed, and a task force approach is being taken to intelligence collection and analysis. Every task force has an open source intelligence specialist, and all requirements for intelligence must first be examined and if possible satisfied through OSCINT before tasking of clandestine or technical capabilities is permitted. More recently, the intelligence elements of the individual military services were integrated into a joint military organization reporting to the Prime Minister.

- Sweden. This country is most interesting because it has a unique consortium within which to formally orchestrate the activities of government intelligence, the business intelligence community, and the university research community. Swedish scientific & technical attaches have been noted to regularly exploit the internet, and there is discussion within Lund University of the need for an Open Source intelligence Center to meet the combined needs of the government, business, and university communities in Sweden.

Advantages and Disadvantages of Open Source intelligence

Advantages include the fact that OSCINT has virtually unlimited potential on any topic; is of relatively low cost because expertise is maintained at someone else's expense; is generally up to date; and can be shared with anyone.

Disadvantages include the possibility of revealing military plans and intentions (security can be provided by laundering the question through trusted intermediaries); the time and cost associated with searching for exactly the right information within the huge volumes of public information; and the temptation to accept an open source at face value when it could be disinformation or simply inaccurate.

Obstacles to Military Exploitation of Open Sources

There are three obstacles to military exploitation of OSCINT:

- Organizationally, the military relies on a classified intelligence community for its "intelligence", and does not have an alternate structure established to obtain OSCINT. Among the most important problems created by this reliance are those of funding: there are no well-established programs for contracting directly with the private sector for OSCINT.
- Culturally, there is a strong attitude, primarily within the intelligence community but to an extent within the operational community, that information achieves a special value only if it is classified. This is in part a result of a cultural inclination to treat knowledge as power, and to withhold knowledge from others as a means of protecting one's power. This attitude is the equivalent of the Calvary ignoring the tank and the machine gun. The "openness" paradigm has thoroughly defeated the secrecy paradigm, and those organizations which focus on protecting secrets rather than exploiting publicly available information, will find themselves "starving" for knowledge.

- Technically, because of the historical focus on training, equipping, and organizing forces for unilateral and conventional military operations, with the added assumption that all "intelligence" will come through classified and well-established channels, the existing command & control architecture, including communications, computing, and intelligence elements, is not designed to rapidly interface with joint and coalition forces, with special forces and direct action clandestine teams, and with the vast array of private sector and non- military government elements which can provide OSCINT to the commander.

Opportunities for Advantage

The Director of Military Intelligence (DM1) for any nation has essentially three opportunities to improve national capabilities to collect, process, and disseminate OSCINT to commanders and military policy-makers:

- Existing library resources are poorly-funded and organized for the purpose of "just in time" archiving of information. Library resources, both within the intelligence community and outside the intelligence community, must be recognized as the "source of first resort"⁶ Commanders and policy-makers must restore funding for library operations, including the cost of subscribing to external online services and out-sourced research, while at the same time redirect the libraries toward "just in time" decision-support to specific consumers, and away from "just in case" generic collection and processing.
- Existing military intelligence analysts must be given the training, fiscal authority, and commander's guidance necessary to convert them from narrow specialists focusing on the analysis of classified information, to managers of networks of overt human experts and related electronic and hard-copy databases. At the same time, analysts must be re-oriented so that their primary focus is on day to day interaction with the commander and other consumers of military intelligence, and on day to day collection management founded upon open source exploitation, rather than the existing focus on producing classified reports in isolation from the consumer.
- Existing commanders, in consultation with the DM1, must recognize that it is impossible for the DM1 to satisfy their intelligence requirements related to a wide range of new priorities, with existing classified military intelligence capabilities. The entire structure of military intelligence must be recast to permit rapid maneuver throughout the private sector's knowledge terrain, and the rapid collection, processing, and dissemination of mission-critical OSCINT to the commander at every level of operations (strategic, operational, tactical, and technical) and in "every clime and place".

Role of the Military Reserve

The military reserve constitute a national resource which has enormous potential. A simple example will serve to make the point. For every country of interest, a cadre of five military intelligence reservists could be formed, and given a responsibility to monitor pertinent foreign language periodicals and publications (which would be provided them on subscription), and to prepare weekly OSCINT summaries. These same individuals should be afforded direct access to the Internet and commercial online databases, and serve as direct

reinforcements on demand to the active duty military intelligence analysts responsible for the same areas of interest. Funds should also be provided for the five person cadre to spend thirty days each in the country of interest, unencumbered by administrative duties. In this way, when a contingency requirement emerges, the responsible commander can activate the appropriate cadre (or cadres in the case of a theater commander).

Endnotes

1. Although the original intelligence community report was classified SECRET, the definition and extensive commentary appeared in an unclassified document, United States Marine Corps Comments on Joint Open Source Task Force Report and Recommendations (Working Group Draft Dated 6 January 1992), and portions, including the definition, were subsequently reprinted in OSS NOTICES Volume 2 Issue 9 (30 November 1994).
2. This point was made publicly by Dr. Stephen Fairbanks, the Iranian Analyst for the U.S. Department of State's intelligence and Research Bureau, in the presence of his superior, Dr. Jennifer Sims, Deputy Assistant Secretary of State for intelligence Coordination.
3. At a Canadian intelligence conference 27-29 October 1994, both the Director of the Canadian Security and intelligence Service, Mr. Ward Elcock; and Dr. Paula Scalingi of the Los Alamos National Laboratory in the United States, stated that OSCINT provides over 80% of the input to the final all-source product; in Dr. Scalingi's case, this was with specific reference to intelligence support for counter-proliferation. Dr. Gordon Oehler, Director of the U.S. Intelligence Community's Nonproliferation Center, has made similar comments on several public occasions.
4. SPOT is going to 5-meter resolution imagery in the very near future. In the U.S. Space Imaging, Inc., a subsidiary of Lockheed, has announced plans to provide 1:2,500 meter synoptic resolution imagery, within a year. These commercial capabilities will be critical to expeditionary operations in the Third World because of the lack of current maps. One U.S. study, Overview of Planning and Programming Factors for Expeditionary Operations in the Third World (Marine Corps Combat Development Command, March 1991), determined that for the 69 countries of concern to the Marine Corps, there were no 1:50,000 combat charts for 22 of the countries, old 1:50,000 charts for ports and capital cities only in the case of another 37 countries, and very old 1:50,000 complete coverage for another ten countries.
5. The extraordinary relevance of Department of Energy OSCINT capabilities in support of military operations are described in SHARING THE SECRET: Open Source intelligence and the War on Drugs (OSS inc. Limited Edition, 1994). The Army paper, prepared by the 434th Military intelligence Detachment, Strategic, is titled Open Source intelligence Resources for the Military Intelligence Officer (Fort Huachuca, November 1994).
6. This important phrase was developed by Mr. Paul Wallner, the first (and last) Open Source Coordinator in the Office of the Director of Central intelligence in the United States. Mr. Wallner, a member of the Senior Executive Service (flag rank) served for many years in the Defense intelligence Agency and has been a strong advocate for improving OSCINT support to the commander. Today he serves as Deputy to the first Director of Community Open Source Program Office, Dr. Joseph Markowitz.

THE PRIVATISATION OF INTELLIGENCE: A WAY FORWARD FOR EUROPEAN INTELLIGENCE COOPERATION - "TOWARDS A EUROPEAN INTELLIGENCE POLICY"

Dr Andrew Rathmell
RAND Europe, <http://www.randeurope.org/>

Introduction

A major objection to increasing international cooperation in the intelligence field is the traditional reluctance of intelligence services to share information on their sources and methods. At the other end of the intelligence "chain," nation states have also been reluctant to rely on their allies for the all source assessments on which, ultimately, political and diplomatic policy are based.

Despite the growth of trans-European intelligence networking, these sensitivities will continue to hamper efforts to improve intelligence collaboration in a European framework. The argument of this paper, however, is that the "privatisation of intelligence" in the developed world will help to break down such barriers to cooperation and provide means by which all European states can benefit from pooling resources. Critically, budgetary pressures will push collaboration while the pull of privatised intelligence will encourage outsourcing and make collaboration easier.

Privatising Intelligence

Intelligence services have always made extensive use of "open sources" - from studying foreign press to debriefing businessmen and tourists and collaborating with academics and scholars. Proponents of the Open Source Intelligence (OSINT) revolution however argue that the intelligence business has been revolutionised at the end of the twentieth century by the information revolution that has generated a flood of data available without recourse to clandestine methods.

This paper accepts that intelligence services can now glean increasing amounts of data from open sources but argues that the privatisation of intelligence for European governments in the 1990s goes further than this. The privatisation of intelligence includes four components: targets, sources, methods and costs.

Targets

The geopolitical changes since the end of the Cold War and changing attitudes to the role of Western military forces and European global security interests have changed the intelligence targets of concern. European agencies must focus on a much wider range of potential targets, all of which are individually of a lower priority than the Warsaw Pact during the Cold War. They must now pay attention to arms proliferation, terrorism, crisis prevention and monitoring and prepare for possible military intervention overseas, whether humanitarian or otherwise. Although certain key issues, such as WMD programmes in certain states or the

activities of certain terrorist groups, will require consistent and in-depth monitoring, other issues will require a broad-brush overview combined with a surge capability.

This broad brush overview can often be provided by open sources (e.g. press, media, individual experts, diplomatic reporting). At the same time, there is a convergence of interests between defence intelligence services on the one hand and criminal intelligence services on the other in the fields of, for instance, organised crime. Both sides of the fence are not only having to learn from each other's experts but are rapidly having to educate their personnel in relation to their new targets. This is the stage at which OSINT and expertise is often the most useful.

Sources

As Robert Steele and others have argued, the information revolution and the proliferation of media and research outlets mean that much of a state's intelligence requirements can today be satisfied by a comprehensive monitoring of open sources. There is little reason to think that this can be done better by in-house experts than by established private sector research institutes and companies. Crucially too, outsourcing will often relieve budgetary pressures.

Not only are open sources now more widely available, but the information revolution is even blurring the boundaries between open and covert sources in regard to the formerly sacrosanct technical collection means. The proliferation of civil Earth Observation satellites and improvement in image analysis techniques are rapidly eroding the monopoly on Imagery Intelligence (IMINT) formerly reserved for the USA, Russia and, to a lesser extent, the PRC.

Methods

The key to good intelligence is all source assessment. While state apparatuses, especially in the major European military powers, have methods and mechanisms that cannot be matched by the private sector, these methods and mechanisms are optimised for certain core missions. Since these methods were designed around Cold War scenarios, they are not necessarily best placed to assess new threats and support new missions. Two areas of note are Operations Other Than War (OOTW) and Information Warfare (IW). The new complex of issues surrounding these contingencies involves less traditional hard military net assessments and diplomatic intelligence, and more soft analysis of complex political, paramilitary, social, economic and technological issues. Since these new issue areas are only now being defined and categorised, more flexible private sector institutions, less locked into established modes of analysis and less beholden to bureaucratic imperatives, can offer a lead in reformulating intelligence methodology for a new era.

Costs

As defence budgets shrink across Europe, armed forces are having to rethink their provision of in-house expertise. Britain has already decided to "privatise" the education of its staff officers in order both to save money and to improve quality. In terms of technology, armed forces are increasingly reliant on off the shelf technology (COTS) while many of the technological advances in the Revolution in Military Affairs (RMA) are now civilian and not military led. These processes are likely to continue; the logical corollary is an increasing reliance on OSINT. Importantly, the low level of classification required for such sources and

methods also enables resources to be pooled between states. This further reduces costs and is likely to improve European coordination in a time of crisis.

Sources and Methods: Satellites and Information Warriors

In order to put some flesh on the skeleton outlined above, this section considers two particular areas in which the information revolution is increasing the role of the private sector. The leading role of the private sector in these areas makes it much easier for European states to collaborate both to improve their intelligence take and to cut costs. First, I will discuss one type of intelligence source, space-based IMINT. Second, I will discuss the methodological issues related to Information Warfare.

The Earth Observation Revolution

A striking feature of modern international relations has been the impact of the dominance exerted by the USA in regard to the provision of satellite IMINT. America's vast investment in its space-based surveillance and reconnaissance infrastructure has given it tremendous influence both diplomatically and militarily. Desire to break out of this hegemony has encouraged some states to pursue their own space-reconnaissance capabilities, such as the Helios and Japanese satellite programmes. Proponents of closer European intelligence collaboration often argue that it is necessary to enable Europe to afford to deploy its own high resolution surveillance satellites. However, the accelerating technical and market revolution in the civil Earth Observation (EO) field is providing capabilities that will soon enable the private sector to challenge the US hegemony in overhead imagery and provide IMINT capabilities unaffordable even with a joint European satellite programme.

The EO Revolution has four key components: Sources of Imagery, Quality of Imagery, Image Processing & Analysis techniques, Developments in Data Integration.

Sources of Imagery: Whereas SPOT and Landsat for many years were the sole commercial providers of imagery, other providers are now emerging. Already Russia and India market high quality imagery, as do Europe and Japan from the ERS and JERS radar satellites. By the turn of the century, perhaps three American companies will be providing electro-optical imagery while Canada will be selling data from its Radarsat. Europe will also be marketing data from its ENVISAT while Japan may market data from its proposed EO satellites. The impact of this proliferation of suppliers is to make data cheaper and data supply more reliable, meeting two of the key requirements of an intelligence service.

Quality of Imagery: Intelligence services are understandably keen to have high resolution imagery and have never considered Landsat, for example, of much significance due to its coarse resolution. The Very High Resolution electro-optical data now being marketed and being proposed means that sub-one metre resolution data will soon be available. This is adequate for most defence tasks. Moreover, the number of EO satellites in orbit and the variety of sensors available (panchromatic, Multi-Spectral, Synthetic Aperture Radar) can provide a level of coverage in terms of repeat times and in terms of elements of the spectral band that not even the US government has achieved.

Image Processing & Analysis techniques: Advances in civil applications of image processing for both electro-optical and radar data mean that more information than ever can be extracted from imagery and that data management issues can also be addressed. While classified

programmes within the US will continue to lead in some of these areas, industry and academia can add significant value to EO data, often at lower cost. In addition to technological developments, the skills and data required for this highly specialised type of intelligence gathering are proliferating into the private sector.

Developments in Data Integration: Overhead imagery can no longer be seen as aerial photo-reconnaissance writ large. The emergence of data integration tools, such as Geographic Information Systems and Digital Terrain Modelling, marks a dramatic advance in the ability to generate maps and terrain models of unknown areas. In light of the probability that European forces will have to intervene at short notice in unfamiliar geographical areas, the benefits for mission planning from GIS and DTM are incalculable. Again, the data sources, the tools and techniques involved are being led by the private sector.

The EO Revolution has profound implications for the privatisation of intelligence and for European collaboration, some of which were recognised with the establishment of the WEU Satellite Centre. High quality overhead imagery will soon be available to all comers combined with greater than ever analytical and mapping capabilities. Although individual national intelligence services will obviously make use of these new capabilities, the fact that the sources and methods are "open" - available commercially, opens the way for them to be exploited collaboratively. This will reduce costs and increase synergy. The fact that these resources are not controlled by any one member state will remove the possibility of any disputes over tasking, as has happened on occasion with Helios.

Information Warfare

Information Warfare is still a contested term and has been given many different meanings. For the purposes of this paper, it is defined as "attacks on, or defence of, information activities." Although targeting an enemy's Command, Control and Communications (C3) is not new, the use of the term IW takes account of the fact that both militaries and states are increasingly reliant on Information Infrastructures to conduct their business. Although physical infrastructures (railway lines, bridges) remain critical, at least as important are critical nodes in Information Infrastructures.

An emerging concern among intelligence agencies therefore is to examine the implications of this reliance by armed forces and societies on networked communications. Even the USA, which has jumped onto the IW bandwagon, has not yet however conclusively defined its approach and methodology. European states have so far paid relatively limited attention to this topic. As they turn their attention to it, they will find it extremely beneficial to look to the private sector in three respects: Conceptualisation, Threat Assessment, Vulnerability Assessment.

Conceptualisation: For better or worse, America's conceptual approach to IW has been shaped by non-governmental "experts," such as the Tofflers. The lack of scholarly rigour evident in such popularised analyses is however widely acknowledged and it is evident that a great deal of hard intellectual work needs to be done in Europe to put IW in context and to develop the conceptual tools without which policy and doctrine will be incoherent and poorly grounded. Although such high level thinking is being done within government circles, there is a place for substantial input from the academic strategic studies community and from the academic/commercial Information Technology community. This early stage of conceptualisation requires a true partnership. At a later stage, when policies are being

implemented, this partnership will need to be formalised and extended. The USA, for instance, has explicitly structured its Computer Emergency Response Team (CERT) concept as a partnership between executive agencies and the private sector. Despite the massive expertise and resources of, for instance, the NSA, it has recognised that a partnership is the only viable option.

Threat Assessment: European intelligence agencies are only now beginning to develop threat assessment methodologies for IW. One pressing problem in assessing the extent and nature of the threat is the lack of data regarding "real-world" IW attacks, as opposed to speculations about the potential IW threat. It is commercial institutions that are in the front line of IW-type attacks, usually for criminal purposes. Government police and intelligence services have however found it very difficult to extract reliable information from companies about the extent of the damage inflicted. The aims of the two sides are often in opposition. Companies are concerned to avoid publicity which will impact on consumer confidence whereas governments are concerned at locating, understanding and neutralising the threats. To resolve this contradiction, there is place for more reliance on privatised intelligence.

For instance, in 1994 King's College carried out a threat assessment for UK-based companies considering the physical threat from the Provisional Irish Republican Army (PIRA). Despite the sensitive nature of the subject, it was established that a combination of research methodologies (strategic analysis and consumer threat perceptions) could usefully generate methods and data of benefit to both government and the private sector. Possibly more importantly, the research process provided a mechanism for improved information exchange between the public and private sectors. This approach could contribute significantly to the development of national and multinational IW threat assessments. An additional area in which privatised intelligence would score over government intelligence is in tracking IW doctrinal and technical developments in other states. For instance, foreign scientists are often more willing to collaborate in research efforts with other universities than with defence agencies or intelligence services.

Vulnerability Assessments: In assessing the vulnerabilities of a National Information Infrastructure (NII) or the Global Information Infrastructure (GII), intelligence services already recognise the prime importance of working with the private sector. No modern government can understand the potential weaknesses in its NII unless it works closely with, for instance, leading IT companies and service providers. These forms of collaborative research need to be extended on an international basis due to the interlinking of NIIs with regional and GIIs.

Implications for Europe

Improved European intelligence collaboration is rational from the perspective of the push, declining budgets require resource sharing, and of the pull, the increased demand for intelligence and the proliferation of sources and methods. Nonetheless, reluctance to divulge sources and methods will act as a brake on intensified collaboration. This paper has argued, however, that the ongoing "privatisation" of intelligence will ease these sensitivities since, in a private-sector led environment, sources and methods will be widely available. Specialised and highly classified collection and analysis methods will remain under official lock and key but the role of classified programmes is likely to be significantly reduced in the near future. In order to benefit from the ongoing information and intelligence revolutions, all European

states could only benefit from closer European collaboration, both between governments and with the private sector.

OPEN SOURCE - LESSONS LEARNED

Mats Bjore

During our early work in the late 1980's we began to realise that the way we access information as analysts had to change. Due to the ever-increasing volume of information, we had to focus our interests.

For every major or minor event in the world there often is at least 20 independent sources that are reporting on the very same event. The risk and possibility of misinformation or deception have grown, but the risk also has been reduced. It had become harder for the remote and closed areas of the world to keep things in secret and to fool it's own citizens with propaganda.

The different media types blend and soon it will be impossible to decide which type of communicator has delivered a certain stream of bits. The television set becomes a computer. You download your e-mail to your cellular telephone. You use your computer to monitor the local TV or radiobroadcast from Israel to Brazil. The satellite dish on your roof is a super high-speed connection to the INTERNET. The change is continuous, simultaneous, accelerated, and nonlinear—in one word: chaotic.

How does an organization organize the monitoring and analysis of events that affect its operations in a rapidly increasing flow of information? They can not attend to every event in its environment, but must select areas of priority, filter incoming data according to its interests, and for further refining and analysis.

One of the major problems today is how to say NO to the quantity of information delivered by emerging push and pull technologies and instead focus on the quality of information needed for analysis. The human interface is still needed.

Our open-source function still acts as a human filter, in order to ensure quality. This has the added benefit of keeping our stored volume of information within reason—thus ensuring our clients relevant and timely retrieval.

History

In 1990 two disparate needs arose that necessitated the use of unconventional sources and methods.

The Swedish Army Parachute Ranger School required pictures and information at the tactical level.

The Army Intelligence School needed open information in its task to disseminate threat assessments. Much of the available information was either classified or not relevant. With open sources, both requirements were satisfied.

One of the incidental lessons learned quickly became known as ASKINT (or Asking Intelligence). There was a need for up-to-date pictures of materiel.

Instead of attempting the traditional covert (time-consuming and very expensive) means of collection, letters were sent out to manufacturers asking for the requisite pictures—ASKINT.

Aerospatiale, among others, promptly sent not six but 53 pictures of its product line. Even the Russians responded: the tank factory in Omsk sent pictures of its latest T-80 model.

In 1993 the Military Intelligence & Security Service realised the need to adopt the methods developed at the Intelligence School, on the strategic level.

At the end of 1996 we introduced our global-access document database the so-called Infobank.

In mid-1997 we became an independent unit within the service.

Our daily work is focused on three major products

The Open Source Information Report, the INFOBANK for the Defense Forces HQ and the GLOBAL INFOBANK for our external customers. Among our external customers we have the MoD, the Foreign Ministry (including many embassies around the world), the National Defence University, the Regional Military Commands, and other members of the Swedish Administration. Infobank is the text collection of all digital OSI collected since 1993. It is indexed both manually and for full text retrieval. We combine the best of two worlds.

Method

The most important task of the day is the routine collection of monitored sources. This is sometimes a very tedious task but it is necessary in order to maintain the quality of our INFOBANK. Our goal is to find and use primary sources

Our team work from several different locations and from their home offices. In The use of LRRP (Long Range Reconnaissance Patrol) tactics is important. Several hours a day the LRRP scans the forefront of the INTERNET or any commercial online-service for new relevant sources and reports and map the location, content and development of valuable sites and services.

They LRRP must have very good knowledge of the organisation's basic needs, full clearance for the content and work of SIGINT and HUMINT in combination with an innate sense or feel of what will become important. This scouting function also serves as a sort of Help Desk for the analyst and the information miners.

Yes we use the human interface. We believe until proven otherwise that the Mark I Eyeball driven by a hungry, curious brain is superior to any binary agent. The Push technology or profiling system, we believe, make the analysts passive and their curiosity for "out of the normal picture" gets drowned in the bitstreams of endless hits in the profiling systems. And a profiling system as of today and the nearest future will only make the active and curious analyst frustrated. He or she want to know more, learn the details and the want do DISCOVER the information by their unique individual way of thinking.

If you are part of a large organisation with many LRRP, it is essential to coordinate pointers to locations to be searched, and to establish procedures to create the organisation's own

source pages- If you do so, you don't waste valuable time in the collection process or duplicate your efforts.

A LRRP must be of an analyst's breed. We tried to use computer whiz kids but in our experience, you must have people with very broad skills and education. **Computer skills are not important but language, sometimes unconventional intelligence and "organisations" skills are essential.**

In addition to the LRRP we use miners that collect the information and structure the information in our system. Structuring means that insight or meaning is obtained by matching and relating information from multiple sources so that some form of pattern or trend emerges. Structuring is achieved by creating information about information, for instance, how data are organised, related and used. Classification, indexes, tables of contents, and data models are some examples of filtering and the structuring of data. Some sort of structuring combined with a sufficient text retrieval system hold the most potential for the successful exploitation of information.

A great deal of important information is present on the net for only a short period of time. When you have identified a specific piece of information, you must capture it and store it in your own system. For as long as you continue to want that information, you continue to monitor the source. If you use a local indexing system, you also get the benefit of having the information searchable and useable.

Although sometimes valuable, **the Internet today is not a solution to the analyst's need for relevant, timely information** The Internet is changing by the minute. New sites appear at a breathtaking rate—one of the major online Internet catalogues receives 22,000 new listings every day. At the same time, many sites go away. Because it only takes a few minutes at a computer to change a site, they change regularly. This means that mastery of Internet information is extremely perishable. **On top of the vast amount of new material entering the Internet, its structure and essence are also changing. The look of the Internet has also changed dramatically. Text-only "gopher" sites are being replaced by graphics-laden and sometimes beautiful "web pages." This transformation will continue for some time.**

New resources and methods appear and others fade away on a daily basis. Within a few years, the web is likely to stabilise. Once that happens the analyst's or the LRRP's collection of Internet ~bookmarks" will be nearly as valuable as personal contacts are now. The modern analyst must prepare for this. By exploring the web today and developing effective methods for finding and using electronic information, the analyst will be ready and competitive when the Internet finally does make the leap from luxury to necessity. But as a manager you probably don't want your analysts to surf away from their given daily assignments.

We have solved this need by giving our analysts free access to the INTERNET at home but not on every workstation at work. Every section has a common resource (our play-station) with a wide range of online service including the Internet. It is important to motivate and tease the analysts to be curious about Open Sources.

The rapid pace of development on the INFORMATION BATTLEGROUND demands a constant R&D effort in an Open Source-based organisation.

Organisations must have constantly evolving and changing systems. These changes may not always be visible to the analyst but the manager of an Open Source system must understand and direct them.

As a metaphor, one can take a photo of river or a rapid. The photo is a frozen projection but is very hard to describe in detail. You can paint a picture or write an essay about the river but you can not imagine how the waterfall will look in detail the next second, minute or decade. The only way to comprehend the flow of water is to dive into the water, follow the currents, and try to master it during the ride.

We think the same applies to Open Source. It is and will be a chaotic ride! You must actively take part in the process to understand the process; to have visions and to create new methods and applications. In these areas, specialised R&D institutions are phenomena of the past.

If you have the resources, you must incorporate the R&D functions in the actual living Open Source-process. Your organisation soon will be a **knowledge-organisation** where changes can be very rapid but invisible in the daily tasks. If everyone can influence his bit of the process, the word **changes** soon will loose its meaning

We focus our collection on primary sources, and only use secondary sources when we have to. Often, however, secondary sources can be helpful in finding primary sources.

By using cheap technology and striving for information quality, we could afford to do mistakes. Our OSI organisation has its origin in tactical military intelligence and the same methods for collecting, structuring, analysing, and dissemination was applied to the operational and strategic level in both the military and in the field of security politics. We learn by trial and error.

For strategic analysts, the ability to collect information rapidly and to evaluate its relevance and validity is a crucial skill.. One of the most important lessons learned is that the end user or analyst must have software that is simple to learn and contains a minimum of "wizard-features". We believe that we must use the same technology and graphical user interface as the analysts share with their children and spouses at home. We learn by socialising with our friends and families.

If you are a cyber soldier or an information scout you are used to—and live in the rapidly changing software battleground.

However, for the analyst, the **need is not survival on the front line** but rather a calm and stable environment for analysing the information and producing intelligence. If you change the operating environment for the analyst too often, part of their days will be devoted to **taming the tool**.

Do not waste their time with unnecessary options and new versions of software until there is a real demand for new options.

As an example: One of the best analytical mind and graphical mind mapping tools we seen so far is Microsoft Encarta with the note an pushpin function. It is not big buck GIS software but it is cheap, easy to use and your children can help you if you get stuck!

Today we still use cheap off-the shelf software, simple and affordable servers and ordinary PC for the end user.

In our organisation we use effective, simple off the shelf tools that also are very inexpensive.

This means that we can afford to make mistakes, to change, to constantly do R&D in the area of text retrieval. If we invest in a high-tech million dollar system that works effectively today, we can not, due to budget restraints invest in next years wizard software.

In our Open Source-centre we take the most relevant and best information from INTERNET and from our other providers and sources -structure and it in a single document base that is accessible with one software tool. The analyst doesn't have to learn the continuously changing retrieval systems. What we do is to create one meta-provider with both an electronic and human interface.

This creates space and time for the analysts main mission. To create knowledge or intelligence out of the information we have collected and structured!

And we must remember one important truth.....

We are competing with the papers and specialists forum around the world. Our decision-makers read the newspapers watch the broadcasts from CNN etc.

We must digest more information in a shorter period of time; **we must reduce the time for transformation from information to intelligence.** The days of status quo are forever gone. And speaking about the media.....

Misinformation

One of the biggest keyword for NOT implementing OSINT in an intelligence process is MISINFORMATION. "The OSI is full of misinformation and attempts of deception"....??? Well that may be true. Nevertheless, it is in the same degree true for both SIGINT and HUMINT.

As an example:

Source A, belonging to a rouge diplomatic mission in one of the intelligence agency target countries, use the telephone frequently. In a conversation with Source A base at home Source A may be saying something like u I have information that the leaders of the subversive European Union have been here discussing R, S and T"

This conversation is intercepted by SIGINT and forwarded to the databank or the archives at the intelligence agency, The conversation is upgraded to state secrets because of the way of collecting not necessarily the content. HOWEVER, the analyst regards the SIGINT information as validated and VERY important.

The fact that SOURCE A may have heard about the meeting in the broadcast of the local radio or read The Economist and then talked about it a couple of days later NOT citing the original source is forgotten.

What do I mean? OSI may have the benefit of teaching cold war analysts and just out from the university the art of looking at every piece of information with the same critical eye regardless if its HUMINT, SIGINT or OSINT.

In my opinion the most valuable characteristic about OSI is

You always know the source, if it is primary or secondary

- It is cheap
- It is fast
- It is available

Some of the key lessons that we have learned are:

- Focus on finding quality primary sources.
- Keep all information in one format.
- Do it simple
- Maintain the human filter.
- Give the analyst only one - simple - tool

And most important of all

Sharing is Power!

OPTIMISING OPEN SOURCE INFORMATION SHARING IN AUSTRALIA: REPORT AND POLICY PRESCRIPTION – (Part IV, V)

**Lieutenant Colonel Ian Wing - 1999
Chief of the Defence Force Scholarship Fellow
Australian Defence Force**

Australia is taking positive steps to optimise open source information (OSI) and open source intelligence (OSINT).

Part Four: OPEN SOURCE SHARING IN AUSTRALIA

Current Australian Arrangements – National Security

The intelligence agencies involved in national security have made progress in the discipline of OSINT over the last few years. The scope and extent of this progress has varied from agency to agency.

DFAT

The Department of Foreign Affairs and Trade operates the Open Source Collection Unit (OSCU) which contributes to the Foreign Broadcast Information Service (FBIS).

Case Study – ASIO (1)

The Australian Security Intelligence Organisation draws heavily on open source capabilities.

ASIO has developed the Intelligence-Based Decision Model (IBDM) and it allows each element of the intelligence ‘business cycle’ to be identified and compartmentalised into workable projects within a strategic planning framework.

Intelligence is only one part of the general policy process and ASIO recognises that its clients receive advice from many other sources, which may differ from ASIO’s advice. ASIO seeks to understand the whole decision-making process: the policy framework; the stakeholders and their expectations; the attitudes of clients; and the real or implied intentions of alternative advice. The intelligence adviser who fails to pay heed to open source material may find that their client has a better idea of the general situation and a set of predispositions that any amount of covertly-sourced material may be unable to shift.

OSI forms a key element of the ‘all-source continuum’ which has several broad characteristics relating to the utility or otherwise of OSI and Covert Source Intelligence (CSI):

Open Source Information	Covert Source Information
Open Access	Closed access
Cheap	Expensive

Reliability unknown	Reliability known
Independent	Dependent
Unstructured	Structured
Low risk	High Risk
Least Intrusive	Highly intrusive
Overt	Covert

In practice the all-source continuum includes three groupings of sources which have hazy boundaries. These are:

- open, publicly available information (such as the media, on-line sources and the Internet);
- restricted access (such as police information, official information and foreign government records); and
- closed and/or covert (such as national security information and protected sources).

ASIO applies a structured approach to security risk management using the Security Risk Matrix (SRM). The SRM consists of:

- Likelihood of Threat x Nature of Consequence = Risk
 - Intent x Capability = Likelihood of Threat
 - Desire x Confidence = Intent
 - Resources x Knowledge = Capability

The hypotheses used by ASIO in the SRM process are generated using OSI . The hypothesis is then tested with additional specific monitoring and limited investigation, and a requirement collection plan is developed. To complete the assessment it may be necessary to access all available sources of intelligence and maintain collection and assessment activity if the security environment is particularly volatile or uncertain.

The ASIO Library provides a significant OSI capability to the organisation. It cooperates closely with other OSI units within the Australian intelligence and law enforcement arenas.

Case Study – DIO (2)

DIO has been officially exploring the utility of open sources since 1995. DIO has an Open Source Unit (OSU) co-located with the Information Centre. The primary open source is the Internet, complemented by participation in the US Government sponsored Open Source Information Service (OSIS), and traditional hard copy library resources. In addition, it has continued to exchange material with FBIS. It receives direct syndicated media feeds, and the DIO 24 hour watch maintains continuous monitoring of the international electronic media.

Their Internet experience suggests that there is a huge and diverse quantity of material (much of it at little cost) but the more useful data-bases and services do require quite substantial subscriptions. A properly trained and equipped unit of specialists is considered more effective than providing Internet access to all-source analysts.

Foreign print media coverage remains limited by translation capacity, but this adds another dimension of support to analysts covering topical geographic issues and crises. Customers will often obtain news reports and they are at times inclined to act upon them. DIO has a particular responsibility to verify the reports and place them into context.

The Open Source Unit, and the 24 hour watch, understand both the intelligence process and current topics of interest. This enables them to add significantly to the all source analysts' work. All of this is being done with material that is significantly less expensive to obtain than that from the more traditional sources. This in turn allows the other collectors to focus their energies on doing things which only they can do - and obtaining information which is not available in the public domain. Indeed, open source material can help better to articulate the true intelligence gaps which Australian classified sources must fill.

The Australian Imagery Organisation, which was raised from within DIO last year, utilises open source commercially available imagery in conjunction with classified imagery and all source intelligence. It produces analytical support products, targeting material, contingency support packages and military mapping products.

A National Intelligence Principle (3)

An important principle relevant to the collection of information by the sources of the Australian intelligence community is that covert collectors do not target information if that information is available through other overt means. Besides the waste of agency resources by unnecessarily duplicating the work of each other, why incur the relatively higher cost of covert intelligence collection, and the associated political risk, if this too is not necessary?

An exception to this principle occurs when doubt exists about the accuracy of information received from overt sources. In such cases, covert intelligence might be sought to provide independent verification.

Current Australian Arrangements - Law Enforcement

In the law enforcement arena, OSINT is an important part of the operation of several federal and state level agencies and police forces.

Case Study – OSCA (4)

The Office of Strategic Crime Assessments observes trends in challenges to strategic law enforcement with significant input from its open source cell. OSCA has never run a 'traditional' in-house library service. Instead, it has access to, and support from, the libraries of the Australian Institute of Criminology, the AFP and the Attorney-General's Department . It uses in-house information professionals to provide dedicated support to its intelligence analysts by facilitating access to information and sources required for intelligence assessment work.

OSCA is tasked with analysing the entire criminal environment - and therefore has a very wide scope to its areas of intelligence interest and information requirements. To be able to put together a comprehensive view of the 'big picture', OSCA needs to be able to draw on a very wide information base for its knowledge of all issues of concern.

Every aspect of OSCA's information collection and management activities is carried out according to systematic, disciplined processes. Comprehensive strategies are devised for the ongoing development and operation of all information services. These are included in an Information Collection and Management Strategic Plan, produced approximately every 18 months. The primary operating principle is that all information - regardless of its source, format, or any other distinguishing feature - is collected and managed according to its value to the organisation.

OSI is essential to OSCA for monitoring the global strategic environment; for 'scanning the horizon' for emerging political, economic, social and technological trends and developments; and providing other general broad contextual information. OSI can provide early warning of emerging issues: by taking small, disparate pieces of information from many different sources (like news media, journals, web sites, etc) and pulling it all together to give a picture of the broader emerging strategic environment. OSI can also give OSCA 'rapid orientation' to new issues. OSCA uses a number of online services, including Reuters Business Briefing, FBIS Online, UnCover Reveal, DIALOG and LEXIS-NEXIS, and the Internet is used in a systematic manner.

OSCA likes to use OSI in its reporting. Where similar information is available from both open and official sources, the open source material will usually be cited. This assists in keeping the security classification of reports as low as possible - thereby facilitating wide dissemination - while at the same time protecting any sensitive intelligence sources and methods.

In 1997, OSCA built the Information Requirements and Intelligence System (IRIS), a Microsoft Access database that allows it to manage knowledge of all information requirements, information holdings, information sources and contacts, and other elements of the OSCA information environment in an integrated manner.

Case Study - CLEICC OSI-SIG (5)

OSCA also has a role in the coordination of the Commonwealth's law enforcement intelligence arrangements - primarily through its chairing of the Commonwealth Law Enforcement Intelligence Consultative Committee (CLEICC). The CLEICC recently established an Open Source Information Special Interest Group (OSI-SIG). With representation from intelligence and information professionals from across the law enforcement and intelligence communities, this group aims to facilitate:

- increased sharing of knowledge and experience of OSI-related issues;
- codification of 'best practice' in OSI activities, where appropriate;
- development of opportunities for cooperative and collaborative OSI activities; and
- the establishment of networks between officers in the community who develop and manage OSI collection and exploitation programs and activities.

The OSI-SIG has already identified an Internet exploitation strategy as one area which may benefit from collaboration. Such a strategy would primarily focus on the community-wide sharing of knowledge of valuable web sites and other Internet-based information resources.

Case Study – ABCI (6)

The Heads of Criminal Intelligence Agencies (HCIA) conference in September 1998 directed that the ABCI prepare a business case for the establishment of a centralised open source unit. This was announced by Paul Roger, Director of Intelligence of the Queensland Criminal Justice Commission, in his paper presented at ‘Optimising Open Source Information’. (7)

The business case proposes that a small open source organisation be raised within the ABCI. It will be responsible to the HCIA and to an Open Source Intelligence Steering Committee.

The open source unit will meet Australian law enforcement requirements for collection and dissemination of open source material. The clients of the open source unit will initially be limited to the agencies that comprise the Criminal Intelligence Agencies. After the unit is established, additional agencies may be included as clients of the open source unit if a need is identified for using the service or on pay for service basis. Outsourcing open source collection to a commercial information broker is an option worthy of consideration.

The establishment of an open source unit provides the criminal intelligence community with an ideal opportunity to market an information brokerage service to other agencies. There is also the potential for the law enforcement unit to become part of a larger unit, and opportunities for networking between other OSI units including the RCMP, EUROPOL and the UK’s Metropolitan Police.

The unit will initially concentrate on providing open source information rather than intelligence. When the unit has found its niche it can then concentrate on four other functions: current awareness briefs; rapid response to reference questions; contacting outside experts for primary research; and coordinating strategic forecasting projects. It will draw on the full range of external open sources, software and services.

The first consideration for implementing a centralised open source unit is determining a budget. Robert Steele has suggested that in the experience of the US intelligence community, no less than 1% of the total organisational budget is required. The detailed business case submission is currently being considered by the Federal Minister for Justice and Customs.

Case Study – New South Wales (NSW) Police Service (8)

The NSW Police Service recently established an OSI Unit to maximise the use of Internet within the Service. The unit evolved from a simple beginning, associated with the creation and maintenance of the ‘Crime Stoppers’ web site on the Internet, which was established in August 1996.

The OSI Unit has a dual role of supporting analysts in the production of strategic assessments as well as providing information relevant to the tactical and operational needs of front line police.

The Service is expanding its approach to ‘intelligence driven policing’. Police at the local patrol level are required to demonstrate how their operations and response procedures are driven by intelligence. Commanders cannot rely solely on personal judgments and hunches about the nature of crime in their areas. Police in all operational commands must make decisions based on analysis of statistical crime data, research of patterns and trends,

demographic and census data, and reliable and credible intelligence reports. To respond to the complexities of the operating environment, police require high quality, relevant information. The electronic open source environment is helping to meet this need.

The State Intelligence Group is the central intelligence entity providing strategic and operational support for the NSW Police Service. Analysts use open source information to conduct research on specific areas of crime such as youth crime, transit related crime, counter terrorism and organised crime. Analysts access news services from Reuters and AAP, media feeds for newspaper, radio and television. The Internet also provides information vital to law enforcement strategic analysis, including government data sets and publications, academic and research papers, commercial information.

On another context, the Internet is being used to share crime information between jurisdictions and to establish contacts with counterparts in law enforcement and criminology departments. Unlike some other intelligence products, the majority of strategic criminal intelligence is unclassified. This enhances the value of the Internet for exchange of information between jurisdictions.

The NSW Police service is the lead agency for the security of the 2000 Olympic Games (ASIO is the lead federal agency) and OSI will enhance its capabilities to meet this important responsibility.

Part Five: POLICY PRESCRIPTION

A Way Ahead

OSINT has the potential to integrate the wealth of sources, software and services from the private sector, with the process of intelligence.

The agencies of the Australian Intelligence Community in their strategic plans and policy groups have identified the need for improvement in the coordination of OSINT. This has been reinforced by the Australian National Audit Office report into the Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games which stated that:

The Olympics will present challenges to ASIO in drawing on new overseas sources for information. It will take time to learn what information is available and how to deal with unfamiliar targets. It is important that processes be developed to maximise the access to sources of material and to avoid duplication of requests by Australian agencies. Access to open source material (eg. Internet and the media) may also be used to supplement other intelligence material. However, overseas experience suggests that the use of open source material can be resource-intensive. ASIO should undertake a thorough assessment of the extent to which this option should be used.

All of the agencies can work together to provide a coordinated OSINT capability. This capability would draw on the strengths of each of the intelligence agencies and create synergies between them, noting that many working relationships and shared efforts already exist in areas such as libraries and information technology.

The synergistic approach to OSINT would be guided by existing national intelligence policy (in the foreign intelligence, security intelligence and law enforcement intelligence fields). It would also develop a system in which the OSINT capabilities of each agency are matched to

its specific needs and shared with other agencies, in accordance with government accountability policies.

A future vision for OSINT is that the proliferation of open source information will enable the creation of a 'virtual intelligence community' in which open information sharing and open source intelligence production is commonplace. The community will include and draw strength from public and private sector entities lying outside the traditional intelligence and law enforcement fields. This development will not replace more traditional covert forms of intelligence collection and production, but it will increase their efficiency.

A future centralised national OSINT capability was foreseen at 'Optimising Open Source Information'. Whilst delegates envisaged the great advantages of such an agency, it was considered such a step would be unlikely to eventuate in the near future without a lifting of the current budgetary and bureaucratic restraints. Instead, significant advantages are likely to be obtained through the establishment of a centralised coordination capability. This capability should be based on shared inputs from the intelligence agencies and a synergistic approach to employing their joint capabilities.

The study of OSINT would be advanced through an 'information audit' across the Australian intelligence arenas, to determine current and expected dependency on OSINT. This would provide a basis for information planning, recognising that significant cost savings may accrue from a strategic shift to OSINT. The results of the information audit could be compared to the OSS benchmarks to ascertain levels of best practice in the field. A whole-of-government Australian operational concept for OSINT and a virtual intelligence community could then be developed. This concept should draw on the experience of other nations in this field.

A future Australian OSINT conference should be convened with the aim of building on the results of the 'Optimising Open Source Information' conference. This future conference could receive official support from the Australian Intelligence Community and should take place in 1999 or 2000 at the latest. The conference could enable detailed discussion of OSINT and include closed sessions to consider the relationship of OSINT with classified sources.

Recommendations

As a result of the deliberations of the 'Optimising Open Source Information' conference it was recommended that:

- The utility of OSINT and its ramifications receive further and continuing examination within the national security, law enforcement and business intelligence communities, with a view to the development of a synergistic and coordinated OSINT capability.
- An 'information audit' be conducted across the Australian intelligence arenas which would determine current and expected dependency on OSINT and inform a whole-of-government operational OSINT concept.
- A future Australian conference on OSINT be convened in 1999 with official support from the Australian Intelligence Community.

Conclusion - Important Issues

This paper has described how Australia is taking positive steps to optimise OSI. Several important issues require further effort to achieve optimum solutions.

First, there is a need for greater awareness and understanding about OSI and OSINT. Some middle level managers remain resistant to the introduction of capabilities which do not possess the normal characteristics of intelligence systems: high cost, high technology and high levels of secrecy. This education and understanding is being provided by conferences, meetings with practitioners from other nations, and by the demonstrable successes being achieved by existing OSI units.

Second, there is a need for greater differentiation between the professions of 'information specialist' and 'information systems/information technology specialist'. The former were once known as 'librarians' and they are the experts at finding information. For this reason, they have the potential to become Australia's OSI specialists. The latter are experts at creating computer-based systems. For this reason they play the important role of facilitating OSI through the employment of technology, but they are not necessarily as well suited to becoming OSI specialists.

Third, the budgetary restraints which operate within the official domain in Australia tend to be resistant to the introduction of new capabilities. This resistance can be overcome if decision-makers are made aware that although OSI and OSINT are not free, they can offer real savings in *overall* organisation expenditure. They can also offer increased coverage of areas of intelligence interest.

And fourth, the stove-piping of intelligence into specific disciplines, based on collection methods or customers, needs to be transformed into a cooperative and multi-disciplinary approach. OSI is likely to provide the circuit-breaker which will facilitate this process. It offers the opportunity to enhance cooperation between agencies and improve overall analytical performance.

The opportunities provided by OSI and OSINT have been recognised by many people working in the Australian intelligence profession. I confidently predict that Australia will make further progress in this field. The experiences of other practitioners in the fields of OSI and OSINT, and particularly those attending this conference, will play an important part in optimising Australian open source information sharing.

References:

1. This section of the paper is derived from 'Open Source Information and the Intelligence Based Decision Model' which was presented by Jason Brown of ASIO, at 'Optimising Open Source Information' 1998.
2. This section of the paper is derived from 'Open Source Applications in Defence Intelligence' which was presented by Major General Bill Crews, Director DIO, at 'Optimising Open Source Information' 1998.

3. This section of the paper is derived from ‘Does Covert Intelligence Have a Future?’ which was presented by Ian Dudgeon, a senior intelligence consultant, at ‘Optimising Open Source Information’ 1998.
4. This section of the paper is derived from ‘When Too Much Information is Barely Enough: OSI and the Office of Strategic Crime Assessments’ which was presented by Dr Grant Wardlaw, Director OSCA, at ‘Optimising Open Source Information’ 1998.
5. Ibid
6. This section of the paper has been developed from ‘Business Case for a Centralised Open Source Information Unit’, ABCI, 27 January 1999.
7. ‘The Requirement for a Law Enforcement Open Source Unit’, paper presented by Paul Roger, Director of Intelligence, Queensland Criminal Justice Commission, at ‘Optimising Open Source Information’ 1998.
8. This section of the paper is derived from ‘OSI in a Law Enforcement Environment’ which was presented by Nola Watson, Director State Intelligence Group, NSW Police Service, at ‘Optimising Open Source Information’ 1998.

OPEN SOURCE INTELLIGENCE

A 'FORCE MULTIPLIER'

Lt Cdr Prashant Bakshi, Indian Navy, Research Fellow IDSA, New Delhi
The Tribune (India), Online Edition June 24, 2001

Intelligence agencies have for long relied on SIGINT (Signal Intelligence), HUMINT (Human Intelligence) and COMINT (Communication Intelligence) for their information-gathering requirements. In recent times, 'open sources' have evolved tremendously to the extent that they are seriously considered a source of intelligence, hence the term OSCINT (Open Source Intelligence).

This can be attributed mainly to the proliferation of information and communication technologies, especially the Internet. Information earlier considered as classified is now widely available — and that too at a mere click of the mouse. For instance, during the recent US-China spy plane debacle, one could effortlessly download satellite images of the EP-3 surveillance aircraft parked at the Lingshui military airfield from the Janes defence website (www.janes.com). Furthermore, one could also learn from the website about a recent upgradation, SSIP (Sensor System Improvement Program), carried out on the aircraft, making it the most sophisticated airborne electronic surveillance asset in the US Navy. With such easy access to vital information, intelligence agencies are slowly but surely accruing more importance to OSCINT.

So, what exactly does OSCINT mean? The US intelligence community has aptly defined the term:

"By Open Source we refer to publicly available information appearing in print or electronic form. Open Source information may be transmitted through radio, television, and newspapers, or it may be distributed by commercial databases, electronic mail networks, or portable electronic media such as CD-ROMs. It may be disseminated to a broad public, as are the mass media, or to a more select audience, such as grey literature, which includes conference proceedings, company shareholder reports, and local telephone directories. Whatever form it takes, Open Source involves no information that is: classified at its origin; is subject to proprietary constraints (other than copyright); is the product of sensitive contacts with US or foreign persons; or is acquired through clandestine or covert means."

OSCINT, however, applies the same fundamentals of traditional intelligence — sifting and analysing information to metamorphose it into unclassified intelligence. Often, such intelligence proves highly invaluable when integrated and validated with other sources, and of course, it needs to be finally given the strategic perspective by experts in the related subject. The advantages of OSCINT are immense and, no wonder, countries like the USA, Israel, Sweden and South Africa have adapted well to this form of intelligence and refer to it as a 'force multiplier'.

The common perception that OSCINT is a recent phenomena centered around the Internet is not quite true. In fact, intelligence agencies have always acknowledged the potential of Open Source Information. Take the case of FAS (Federation of American Scientists), a privately funded organisation, which was originally founded in 1945 as the Federation of Atomic Scientists. Over a period of time, it has evolved into one of the most comprehensive resources for Open Source Intelligence — conducting analysis and doing advocacy on a wide range of issues, which include science and technology, national security, nuclear weapons, arms sales,

biological hazards and space policy. If you are searching for information on Pakistan's nuclear reactors or an update on the Chinese cruise missile programme, a visit to their website (www.fas.org) would in all certainty overwhelm you with the kind of information that is available.

Even during the height of the Cold War, some 20 per cent of the information collected by the Americans on the erstwhile Soviet Union came from open sources. A case in point is the Foreign Broadcast Information Service (FBIS), a US government office chartered to monitor foreign (non-US) open source information for use by the US Government.

The FBIS offers an extensive, in-depth collection of translations and transcriptions of Open Source Information from around the world on diverse topics that include military affairs, politics, environment, societal issues, economics, and science and technology.

Today, there is no dearth of OSCINT sources. While most of them (see table) can be accessed on the web, companies like Janes, apart from having an online presence, also publish periodical reports and reviews that are available on subscription. In fact, the Janes annual books on aircraft, ships and weapon systems are nothing short of defence encyclopaedias that are extremely popular in defence libraries all over the world.

Amongst recent OSCINT sources, Stratfor (Strategic Forecasting) and OSS (Open Source Solutions) deserve due mention. While Stratfor started off as a think-tank; it earned due recognition during the conflict between NATO and Yugoslavia with more than 2 million people visiting the Stratfor website. Based in Austin, it has an experienced staff who strive hard to combine intelligence analysis with the rigours of journalism. Subscribers to Stratfor have a host of options — daily global updates to monthly reports — to choose from, and more so at the convenience of receiving it on one's desktop computer as an e-mail.

The OSS, on the other hand, is one of the world's first information merchant banks' practicing information arbitrage and delivering Open Source Intelligence consulting and services. Interestingly, the 'OSS has a unique feature called MindLink that allows members to join discussion lists dedicated to intelligence related topics. It also provides access to over 5,000 pages of material and two publications, a monthly *OSS Notices* and, a quarterly *Global Intelligence Journal*.

In the Indian context, the concept of OSCINT is still evolving; there are a few defence-related websites — bharat-rakshak.com and stratmag.com — that have sufficient ground to cover and be in the same league as their western counterparts. However, there are some news services like POT (Public Opinion Trends Analyses and News Services) which cover various issues in South Asia and publish bulletins on a regular basis.

Surprisingly, one hears more about occurrences of corporate espionage than military espionage, which can be attributed to the cutthroat competition among business conglomerates. This has led to a spurt in companies dealing with business and economic intelligence.

Future indicators convey a vast potential for OSCINT. However, it is unlikely that it would ever replace traditional clandestine techniques — spies and satellites. Open Source has a distinct advantage, that it is always readily available, as in the case of the Gulf War wherein CNN newscasts were potentially more useful to the first US planes over Baghdad since

classified information did not reach on time. Technology is changing at an amazing pace and hopefully advances in artificial intelligence techniques and development of information agents or 'bots' might make sifting and analysing data simpler and less time consuming. Whatever form it may take, technology would always be the means to an end; and not the end in itself.

REFERENCES

COLLECTION AND USE OF OPEN-SOURCE INTELLIGENCE

Compiled by J. Ransom Clark, The Literature of Intelligence
<http://intellit.muskingum.edu/>

▶Aftergood, Steven. "Intelligence and the Open Source Challenge," *Secrecy News* (from the FAS Project on Government Secrecy), 2 May 2001.

According to the "Strategic Investment Plan for Intelligence Community Analysis," produced by the National Intelligence Production Board (NIPB), "[t]he NIPB has made the development of an Intelligence Community strategy for open source a top priority for investment and concerted action over the next few years." In addition, the Intelligence Community "also needs to exploit the Internet and other open media more effectively and efficiently."

▶Betts, Mitch. "Agents Spy Internet Data." *Computerworld* 28 (1 Aug. 1994): 1, 101. Comments from Joseph Markowitz, "director of the CIA's Community Open Source Program Office," on Intelligence Community components hooking up to the Internet "to collect and share 'open-source,' or unclassified, information." On the use of open-source information generally, Markowitz states: "The creation of our office is a recognition that open sources are a valuable resource. As we draw back in some parts of the world, our office provides an information safety net."

▶Bowen, Wyn. "Open-Source Intel: A Valuable National Security Resource." *Jane's Intelligence Review*, 1 Nov. 1999.

This article first offers "definitions of open-source information (OSINF) and open-source intelligence (OSINT). This is followed by a consideration of the utility of open sources in terms of complementing classified information. The article then proceeds with a brief conceptual consideration of the key steps in setting up and operating an open-source collection system. Key issues and problems associated with open source collection are subsequently highlighted. Finally, to provide an idea of the availability and scope of open sources with relevance to national security, some examples related to monitoring proliferation threats are provided."

▶Clift, A. Denis. "National Security and National Competitiveness: Open Source Solutions." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 25-28.

Chief of Staff, DIA, from July 1991.

▶Cote, Maureen. "Translation Error and Political Misinterpretation." *Studies in Intelligence* 27, no. 4 (Winter 1983): 11-19.

▶Dandar, Edward F., Jr.

1. "Open Source Info." *INSCOM Journal*, Jan.-Feb. 1997, 16ff. [<http://www.vulcan.belvoir.army.mil/BackIssues/JanFeb97/janfebpage16.htm>]

2. "Open Source Information Strategy." *INSCOM Journal*, May-Jun. 1997, 32ff. [<http://www.vulcan.belvoir.army.mil/BackIssues/MayJun97/MayJunPage32.htm>]

The main thrust of these two articles is articulated in the following excerpt: "Intelligence experts must continue exploring ... open source information acquisition and exploitation alternatives, such as the use of commercial vendors, universities and military reservists. The intelligence community should explore simultaneous employment of these resources. These external internal community assets are uniquely capable of handling the information explosion and support a number of intelligence community and military core business areas."

Clark comment: It is instructive that neither article mentions existing Intelligence Community resources for the acquisition and processing of open-source information. The suggestions for enhancing Community access to open sources clearly have been influenced by Robert D. Steele (see below) of Open Source Solutions, Inc., whose assistance is recognized at the conclusion of the second article. Although I have nothing but respect for Mr. Steele's entrepreneurial spirit and acumen, he is not the first person to discover the value of open-source material (the predecessor organization of the CIA's Foreign Broadcast Information Service predates World War II). Whether intelligence decisionmakers should move away from long-established and cost-effective governmental open-source collection and management resources toward private-sector-generated materials is worthy of some debate.

►Friedman, Richard S. "Open Source Intelligence." *Parameters*, Summer 1998, 159-165. <http://carlisle-www.army.mil/usawc/Parameters/98summer/sum-essa.htm>.

Friedman's essay "explores the significance of a trend toward increased recognition of the role of open source information and discusses what this may mean for intelligence consumers at every level."

►Gwynne, Sam C. "Spies Like Us: The Internet Is Changing the World's Most Dangerous Game." *Time*, 25 Jan. 1999, 48.

Clark comment: If you can get beyond the silly (and incorrect) title (there are plenty of games in which there have been more deaths than the spy business), this article is about the growth of the use of open-source intelligence in the business world.

"[T]he World Wide Web has given birth to a whole industry of point-and-click spying. The spooks call it 'open-source intelligence,' and as the Net grows, it is becoming increasingly influential.... Among the firms making the biggest splash in this new world is Stratfor, Inc., a private intelligence-analysis firm based in Austin, Texas. Stratfor makes money by selling the results of its sleuthing (covering nations from China to Chile) to corporations like energy-services firm McDermott International. Many of its predictions are available online at www.stratfor.com."

►Holden-Rhodes, J.F.

1. *Sharing the Secrets: Open Source Intelligence and the War on Drugs*. Westport, CT: Praeger, 1997.

According to **Turner**, *IJI&C* 12.1, this work presents a brief, "useful[,] and instructive" critique of U.S. anti-drug policies and activities. However, the author "ultimately falls short" on

his promise to show how open-source intelligence can be made
"a fundamental part of the drug war."

2. "Unlocking the Secrets: Open Source Intelligence in the War on Drugs." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 67-71.

This is a succinct presentation of some of the thoughts that the author develops in his *Sharing the Secrets* (see above).

▶Hutchinson, Robert. "Rumor of War: An Information Vendor's View of the Provision of Open-Source Data in an Unstable World." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 33-36.

Hutchinson is an editor of *Jane's*.

▶Loeb, Vernon. "Back Channels: The Intelligence Community -- Non-Secrets." *Washington Post*, 1 Feb. 2000, A13. [<http://www.washingtonpost.com/>]

According to Robert D. Steele, former CIA operations officer and chief executive of Open Source Solutions Inc., "three of the Pentagon's joint commands have appointed action officers to manage the collection of openly available, non-secret intelligence.

"There is growing interest among the theater commanders-in-chief in operationally oriented open-source intelligence," Steele said. "The continuing difficulties faced by the CINCs in obtaining timely intelligence, including commercial imagery, from the Beltway bureaucracies have led them to begin creating their own direct-access capabilities for open-source intelligence."

See Steele, Robert David, below.

▶Loeb, Vernon. "Spying Intelligence Data Can Be an Open-Book Test: Firm Finds a Market for Publicly Available Information." *Washington Post*, 22 Mar. 1999, A17.

Robert D. Steele, chief executive of Open Source Solutions Inc., in Fairfax, Virginia, "thinks there is one aspect of the intelligence game that he plays better than his former employer: gathering up publicly available information." Steele and his partner, Mark Lowenthal, "don't contend that open sources can replace clandestine human and technical sources. But the intelligence agencies exhibit a bias for their own secrets, they say, and lack internal systems for fully mining business experts, academic authorities, scientific journals, foreign government reports and burgeoning commercial databases, not to mention the Internet."

See Steele, Robert David, and Lowenthal, Mark, below.

▶Lowenthal, Mark. "Open Source Intelligence: New Myths, New Realities." Available at: <http://www.defensedaily.com/reports/osintmyths.htm>. *Intelligencer* 10, no. 1 (Feb. 1999): 7-9.

This is an excellent analysis of the problems surrounding the collection and use of open-source intelligence in the information world of today.

The author argues that the Community Open Source Program Office (COSPO), "the IC's attempt to arrive at a more coherent approach to the open source issues, both technology and content," failed to achieve its mission. The reasons for that failure can be found an "in-grained" Intelligence Community "prejudice ... against open sources," and an overemphasis on "finding an ever elusive technology that would solve the open source problem of multiple and diverse sources."

▶McGill, G.M. (Mert) "OSCINT and the Private Information Sector." *International Journal of Intelligence and Counterintelligence* 7, no. 4 (Winter 1994): 435-443.

"The amount of information available electronically through open sources, information with countless intelligence applications, is staggering.... The

intelligence community must take advantage of every possible resource at its disposal, including the wide array of open source information that is readily available and relatively inexpensive." The author's primary suggestion is for the government to release information in "raw" form through a network like the Internet; private-sector information providers would, then, package or add value to this data.

▶Sigurdson, Jon, and Patricia Nelson. "Intelligence Gathering and Japan: The Elusive Role of Grey Intelligence." *International Journal of Intelligence and Counterintelligence* 5, no. 1 (Spring 1991): 17-34.

▶Steele, Robert David

Robert David Steele is a former intelligence officer and President of Open Source Solutions, Inc., who has established himself as the leader in developing and propagating "private enterprise intelligence." He argues essentially that U.S. intelligence reform is needed, that reform should seek to maximize the use of open-source intelligence, and that the private sector can meet a high percentage of U.S. open-source intelligence needs at a reduced cost to the U.S. Government.

Other articles by Steele can be found under the "Reform" heading and at the web site maintained by Open Source Solutions, Inc.: <http://www.oss.net/>.

See (above) Vernon Loeb, "Spying Intelligence Data Can Be an Open-Book Test: Firm Finds a Market for Publicly Available Information," *Washington Post*, 22 Mar. 1999, A17.

1. *On Intelligence: Spies and Secrecy in an Open World*. Fairfax, VA: AFCEA International Press, 2000.

From "**Publisher's Foreword**": "[T]his compendium of material on understanding the power of open sources [is offered] in the hope it will help chart the new course -- a new model -- for the future of intelligence."

Clark comment: This work brings together many of the thoughts on the state of U.S. intelligence and proposals for reform that have animated Steele's activities for the past decade. The author's hypothetical Senate Bill S.2001 makes hamburger of many sacred cows, but Congress has refused to act on much less radical measures. A terminology quibble: While I fully understand the need for breaking old molds, the title Director-General (as in, Director-General of National Intelligence) sounds more French than American.

While acknowledging that the author and his views remain controversial, **Jonkers**, *AFIO WIN* 19-00, 12 May 2000, finds that Steele's book "contains ideas to which we should pay attention. His vision, leading up to the 'virtual intelligence community' is worth consideration."

Steele provides the following thoughts on his work: "With a foreword by Senator David L. Boren, sponsor of the 1992 intelligence reform legislation, and blurbs from Alvin Toffler, Bruce Sterling, former DDCI Dick Kerr, and flag officers from Russia, Germany and the United Kingdom, this book is unique in that it provides an itemized list of U.S. Intelligence

Community budget cuts totalling \$11.6 billion dollars a year; and completely outlines 14 major new initiatives for restructuring, enhancing, and considerably expanding our concept of 'national intelligence'. With a 50-page annotated bibliography that integrates Silicon Valley, Internet, management, and hacking books with the more traditional literature; a 62-page index; and 30 pages of proposed legislation, the National Security Act of 2001, this is a reference work."

2. "The Importance of Open Source Intelligence to the Military." *International Journal of Intelligence and Counterintelligence* 8, no. 4 (Winter 1995): 457-470.

"In general terms, OSCINT has significant potential as a source of intelligence support for indications and warning, policy development, contingency planning, security assistance, weapons acquisition (design and countermeasures), joint and coalition operations, and tactical operations against new priorities such as proliferation. Finally, OSCINT is vital as a means of rapidly orienting a commander and serving as the foundation for collection management within the traditional intelligence disciplines." (p. 459)

3. "National Intelligence and Open Source: From School House to White House." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 29-32.

4. "Private Enterprise Intelligence: Its Potential Contribution to National Security." *Intelligence and National Security* 10, no. 4 (Oct. 1995): 212-228.

"The aim of this essay is to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to make an inventory of some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.... [I]t is clear that OSCINT can meet the vast majority of America's intelligence needed against the emerging threats, and that OSCINT must be foundation upon which we completely restructure our classified capabilities."

The paper from which this article is derived, given at a conference on "The Producer/Policy-Maker Relationship in a Changing World," 29 October 1994, in Ottawa, is available at: <http://www.oss.net/Papers/training/Lesson001Handout1B.html>.

5. "Open Source Intelligence: What Is It? Why Is It Important to the Military." *American Intelligence Journal* 17, no. 1/2 (1996): 35-41.

"At this time the U.S. military does not have timely broad access to a full range of open sources." (p. 39)

6. "Smart People, Stupid Bureaucracies: A Tough Love Look at U.S. Spies, Satellites, and Scholars." 21 Dec. 1999.
<http://www.oss.net/Papers/white/SmartPeople.doc>.

"In a complex world where billions of people live on \$1 a day and yet have access to radios and televisions that depict the USA as 'the enemy'... we need to be seriously concerned about both the lack of public understanding of national intel, and the relatively pedestrian level of discussion that is found in major media and 'think tank' outlets. This article ... seeks to outline several common misunderstandings, to summarize the findings of the [18-20 November 1999] conference led by President Bush, and to outline fourteen areas where substantial improvements are required if our national intelligence community is to be effective in protecting America in the 21st Century. I would emphasize my belief that a renaissance of our secret national intelligence is necessary, while also stressing that a revitalization of this essential national capability cannot take place in a vacuum -- we must do better at scholarship and must be much more effective and honest in our corporate communications pertaining to real world issues. More fundamentally, our people -- our public and our press -- must understand the great importance of our classified national intelligence community to national security, and must also understand the larger context within which this intelligence community contributes to the intelligence qua 'smarts' of the nation as a whole."

The slides and planned text of the original presentation of Steele's "fourteen areas where substantial improvements are required," made to a meeting of government and industry managers of intelligence on 16 September 1999, are available at <http://www.oss.net/Papers/white/TOUGHLOVE.ppt>. "A longer document with detailed evaluations and financial recommendations is available at <http://www.oss.net/OSS21>."

▶ Studeman, William O. [ADM/USN] "Teaching the Giant to Dance: Contradictions and Opportunities in Open Source Information within the Intelligence Community." *American Intelligence Journal* 14, no. 2 & 3 (Spring/Summer 1993): 11-18.

Remarks made at Symposium on "National Security and National Competitiveness: Open Source Solutions," McLean, VA, December 1992.

▶ U.S. Central Intelligence Agency. *Preparing U.S. Intelligence for the Information Age: Coping With the Information Overload*. Washington, DC: 1993.

Surveillant 3.2/3: "The Scientific and Technical Committee (STIC) Open-Source Subcommittee ... believes there is an urgent need to develop automated tools for coping with information overload. The report gives an awareness of the extent of the problem."

▶ Wallner, Paul F. "Open Sources and the Intelligence Community: Myths and Realities." *American Intelligence Journal* 14, nos. 2 & 3 (Spring/Summer 1993): 19-24.

DIRECTORY OF RESOURCES

**Excerpt from “Open Source Exploitation: A Guide For Intelligence Analysts”,
produced by Open Source Publishing Inc. (<http://www.osint.org/>)
for the Joint Military Intelligence Training Center (JMITC)**

A

Alexa – <http://www.alexa.com/>

Alexa is an interesting project that is attempting to archive the Web while at the same time providing a means for collaborative filtering. The Alexa software creates a toolbar at the base of your browser which gives you information about the site that you are visiting and a list of suggested Web sites on the same topic. The toolbar also allows the user to access the Alexa Web archive.

About.com – <http://www.about.com/>

This search engine/service uses volunteers who are screened by About.com to ensure their expertise in the topic area they edit. Each About.com “GuideSite” is devoted to a single topic, complete with site reviews, feature articles and discussion areas.

AltaVista – <http://www.altavista.digital.com/>

A very fast and popular search engine created by Digital Equipment Corporation. Both Web and Usenet newsgroup content can be searched. Because of the size of its index, you should learn the advanced-search syntax for this engine to generate only the results you seek. Instructions for search syntax can be found on Altavista's home page.

Analyst’s Notebook – <http://www.i2inc.com/>

The Analyst's Notebook is data visualization software that assists analysts by locating, interpreting and displaying complex information in easily understood chart form. The Analyst’s Notebook provides: association (link analysis) charts, commodity flow charts and timelines.

B

Bigfoot – <http://www.bigfoot.com/>

This site is designed to help you find e-mail, telephone and physical addresses. By providing information such as first and last names and state of residence, you can often find an individual's contact information.

BotSpot – <http://www.botspot.com/>

A portal site dealing with information robots (frequently called “bots”), spiders, wanderers, etc. An excellent site for individuals who are interested in the application of artificial intelligence to the Internet.

BullsEye – <http://www.intelliseek.com/>

A software tool that scans the most popular search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. BullsEye also allows you to track changes to a site and provides a workgroup compatible interface. See also Copernic, LexiBot, OS-Mosis, SearchPad and WebFerretPRO.

C

Copernic 2000 – <http://www.copernic.com/>

A free software tool that scans the most popular search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. Copernic also searches Usenet groups and email directories. Enhanced Plus and Pro versions of Copernic are available for a fee. See also BullsEye, LexiBot, OS-Mosis, SearchPad and WebFerretPRO.

D

Deja.com – <http://www.deja.com/>

This search tool indexes the contents of the more than 20,000 Usenet newsgroups. It is the most complete index of these newsgroups. Now run by Google.

Dogpile – <http://www.dogpile.com/>

An excellent meta search engine that is sophisticated enough of to allow the user to enter limited Boolean operators.

E

EuroSeek – <http://www.euroseek.net/>

Europe's premier search engine that supports searches in 40 languages.

Excite – <http://www.excite.com/>

A search engine which indexes Web sites and Usenet newsgroups. Excite attempts to do some analysis of your query terms in an attempt to find relevant sites even if they do not contain the exact terms you enter. Excite also offers a free news profile delivery service based on user-supplied keywords.

F

FAST Search – <http://www.alltheweb.com/>

The FAST Search Engine (Fast Search and Transfer) was originally a research project of the Norwegian Institute of Technology. FAST also contains links to popular search queries such as FTP and MP3. This search engine's owners are attempting to index one billion Web pages within the coming year.

Foreign Military Studies Office – <http://call.army.mil/call/fmso/fmso.htm>

The Foreign Military Studies Office (FMSO) assesses regional military and security issues through open source media and direct engagement with foreign military and security specialists to advise Army leadership on issues of policy and planning critical to the US Army and the wider military community. FMSO and its top notch military experts provide the Intelligence Community and DoD with excellent open source reporting.

Four11 – <http://www.four11.com/>

This site is a search engine designed to find e-mail and physical mailing addresses. Four11 also provides a telephone number search capability.

G

Google – <http://www.google.com/>

Google uses a complicated mathematical analysis to return high-quality search results. This analysis allows Google to estimate the quality, or importance, of every Web page it returns.

H

Highway61 – <http://www.highway61.com/>

This meta search site passes your query to seven major search engines. The combined results are presented in a single window, ranked by the number of sites on which the term was found and the ranking provided by each search engine.

HotBot – <http://www.hotbot.com/>

A search engine which indexes both Web and Usenet newsgroup content. This site offers a wide range of powerful search options including searches by geographic region. Queries are constructed using a graphical interface.

I

infoGIST – <http://www.infogist.com/>

infoGIST offers a wide variety of software applications that provide enhanced search and retrieval capabilities for the Web, intranets, LANs, subscription services, and your computer.

Infoseek – <http://www.infoseek.com/>

A search engine which indexes Web sites and Usenet newsgroups. Company and e-mail address lookups are also supported. This engine provides a rich set of indexed databases for searching.

ISYS – <http://www.isysdev.com/>

A number of text indexing and Internet related software packages that provide a very user-friendly interface. Also sells software for digitizing hardcopy documents and “spiders” for indexing external/internal Web sites. ISYS also allows the user to publish to the Web via its own search engine or to a searchable CD-ROM. See also ZyImage.

L

LexiBot – <http://www.lexibot.com/>

A search tool that does an extensive search of the Internet by leveraging search engines and Web databases. LexiBot uses a multi-threaded design, allowing it to make dozens of queries simultaneously. Documents are retrieved and prioritized for each search result. A free 30-day trial version of the software is available for downloading. See also BullsEye, Copernic, OS-Mosis, SeachPad and WebFerretPRO.

Lycos – <http://www.lycos.com/>

Lycos is a powerful search engine that indexes Web content. Lycos is very fast and has a number of useful features to help refine a user’s search.

M

MetaCrawler – <http://www.metacrawler.com/>

This meta search site searches nine different search engines. Query results are returned ranked by relevance on a single screen.

Microsoft Internet Explorer – <http://www.microsoft.com/>

One of the two most popular World Wide Web browsers that are available free for personal use. See also the Netscape listing.

MSN Web Search - <http://search.msn.com/>

A popular Internet search engine that has an excellent help section.

N

NBCi – <http://www.nbc.com/>

A relatively new portal that includes a search engine formerly known as Snap.

Snap is a search engine that features content from over 100 leading Web publishers. The heart of NBCi portal services is a directory of Web sites and over 500 resource centers, built by a team of editors and reviewers.

Netscape – <http://www.netscape.com/>

One of the two most popular World Wide Web browsers that are available free for personal use. See also the Microsoft Internet Explorer listing.

Northern Light – <http://www.northernlight.com/>

Currently the largest of the Web search engines. Search results are combined with Northern Light's Special Collection documents that comprise 5,400 full text information sources. Access to the Special Collection documents requires a credit card.

O

Open Directory Project – <http://www.dmoz.org/>

A search engine/service that emulates the Yahoo! concept of categorization. The Open Directory Project uses volunteers to provide the bulk of the Web categorization functions. Search engines like Lycos and Hotbot also utilize Open Directory Project's categorization.

OS-Mosis – <http://www.os-mosis.com/>

An excellent Web search tool that allows the user to create and populate a database using a simple floating toolbar. The toolbar allows the user to capture and categorize information from a Web browser or word processor. Users are able to capture images, create categories and automatically acquire URLs and individual Web pages. OS-Mosis then creates a Web site from the user's database in a number of different layouts and configurations. A multi-user version is now available to help organizations manage their open source acquisition efforts. See also BullsEye, Copernic, LexiBot, SeachPad and WebFerretPRO.

P

ProFusion – <http://www.profusion.com/>

Profusion was recently purchased by Intelliseek the makers of BullsEye. ProFusion is a meta-search engine allowing you to query numerous search engines simultaneously. It also allows you to save your searches for later retrieval.

S

Search Engine Watch – <http://www.searchenginewatch.com/>

A Web portal dedicated to information about search engines. If you're interested in keeping track of the ever-changing world of search engines, this site is among the most complete of resources on the topic.

Search Engines Worldwide – <http://www.twics.com/~takakuwa/search/search.html>

Search Engines Worldwide provides an exhaustive listing foreign search engines organized by country or region. As US based search engines rarely index foreign language Web pages, this is an excellent resource.

Subject Search Spider (SSSpider) – <http://www.kryltech.com/>

Subject Search Spider is software that allows you search the Web by querying dozens of search engines simultaneously. Results are displayed through relevance ranking with duplicate Web sites automatically removed. You can also store your searches locally for later viewing.

SYSTRAN – <http://www.systransoft.com/>

The SYSTRAN site offers free access to its machine translation software that automatically translates text or entire Web pages from French, German, Italian, Portuguese and Spanish into English. It can also translate from English into the aforementioned languages. Far from a perfect translation, SYSTRAN does provide a good enough translation to enable the user to get the gist of the article or text.

T

Teleport Pro – <http://www.tenmax.com/>

One of the better off-line browsers that allows you to duplicate Web site data for fast offline access.

U

Usenet Groups

Usenet groups are electronic discussion lists similar to electronic bulletin boards. Users subscribe to a Usenet group to engage in or read about a discussion with other users. Each Usenet group is focused on a particular topic be that politics, medicine, religion, current events, etc. For search engines that index Usenet groups see also the Deja.com and Altavista listings.

W

WebFerretPRO – <http://www.ferretsoft.com/>

A software tool that scans approximately 30 search engines and delivers hit results and descriptions to the user. The results can be saved for future reference or review. The Power User Pack also searches Usenet groups, current news, e-mail addresses and telephone listings. See also BullsEye, Copernic, OS-Mosis and SearchPad.

Wisdom Builder – <http://www.wisdombuilder.com/>

A text indexing/link analysis/data visualization tool that allows you manage and manipulate large volumes of data. Wisdom Builder also markets its Gold Rush search software that is an artificial intelligence-based meta "find" engine that focuses on extremely high quality search results in a natural language processing based search environment. A free 30 day trial version of Gold Rush is available for downloading.

Y

Yahoo – <http://yahoo.com/>

This service provides a directory of sites screened by staff reviewers. It is an excellent place to start a search, although does not add new Web sites as frequently as most other search engines. If the Yahoo directories do not provide relevant sites, you will be referred to other search engines.

Z

ZyImage – <http://www.zylab.com/>

An excellent text indexing, archival and dissemination software package that allows the user to digitize large volumes of paper documents or electronic files. ZyImage also allows the user to publish to the Web via its own search engine or to a searchable CD-ROM. See also ISYS.