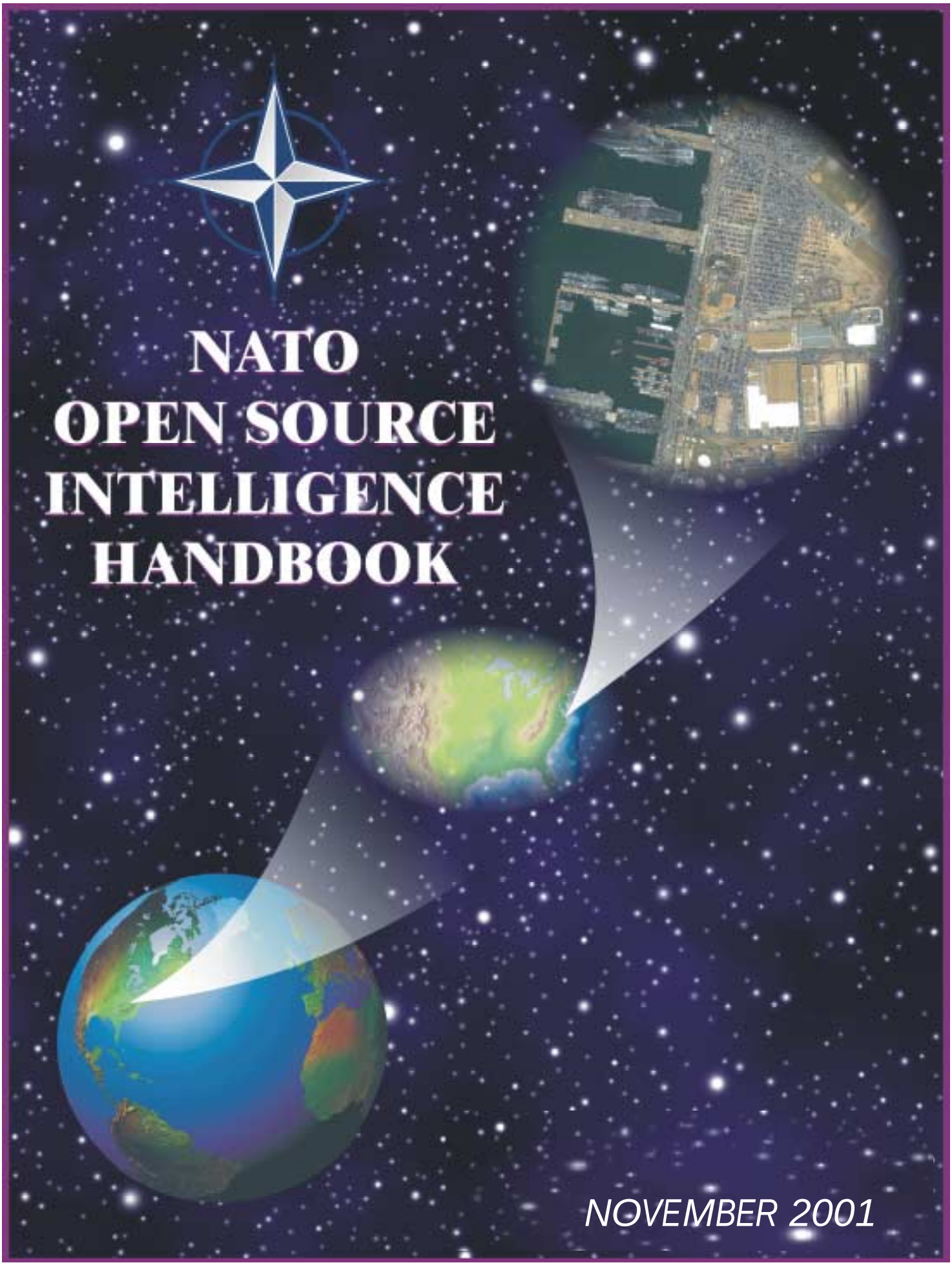

NATO
OPEN SOURCE
INTELLIGENCE
HANDBOOK
NOVEMBER 2001

This Page Is Intentionally Left Blank

PREFACE

This publication provides preliminary joint and coalition training information on the subject of Open Source Intelligence (OSINT). It discusses the fundamentals of OSINT support to both the all-source intelligence process, and to the unclassified intelligence requirements of operators, logisticians, and civilian organizations participating in joint and coalition operations. The focus is on relevant information that can be obtained legally and ethically from the public and private sector, and that is not classified in its origin or processing. The information may become classified in relation to the commander's intent or its association with classified information when it is rightly blended into all-source intelligence reports.

This publication has been prepared under my direction as the Supreme Allied Commander, Atlantic, in collaboration with staff from the Supreme Allied Commander, Europe (SACEUR). This publication has benefited greatly from the continued collaboration between my staff and the staff of Open Source Solutions Inc. With the publication of this document and its companions, the *Intelligence Exploitation of the Internet* and the *NATO OSINT Reader*, commanders and their staffs will have basic guidance for the development of OSINT.

The increasingly robust array of open sources available to all staffs enable commanders at all levels to attempt to satisfy their information requirements themselves rather than immediately directing Requests for Information (RFIs) elsewhere. This manual outlines a systematic approach to OSINT exploitation.

This information 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.

W. F. KERNAN
General, U.S. Army

This Page Is Intentionally Left Blank

Table of Contents

EXECUTIVE SUMMARY

COMMANDER'S OVERVIEW

Open Source Intelligence (OSINT) in Joint and Coalition Operations

Open Source Intelligence, or OSINT, is unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question. It provides a very robust foundation for other intelligence disciplines. When applied in a systematic fashion, OSINT products can reduce the demands on classified intelligence collection resources by limiting requests for information only to those questions that cannot be answered by open sources.

Open information sources are not the exclusive domain of intelligence staffs. Intelligence should never seek to limit access to open sources. Rather, intelligence should facilitate the use of open sources by all staff elements that require access to relevant, reliable information. Intelligence staffs should concentrate on the application of proven intelligence processes to the exploitation of open sources to improve its all-source intelligence products. Familiarity with available open sources will place intelligence staffs in the position of guiding and advising other staff elements in their own exploitation of open sources.

Open Source Intelligence and Joint or Coalition Operations

OSINT is a vital component of NATO's future vision. Through its concentration upon unclassified open sources of information, OSINT provides the means with which to develop valid and reliable intelligence products that can be shared with non-NATO elements of international operations. Experience in the Balkans, and the increasing importance of the Partnership for Peace and Mediterranean Dialogue members in security dialogue, illustrates the need to develop information sources that enable broader engagement with these vital partners.

Private Sector Information Offerings

The Internet is now the default C4I architecture for virtually the entire world. The principle exceptions are most militaries and intelligence organizations. The Internet facilitates commerce, provides entertainment and supports ever increasing amounts of human interaction. To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias and reliability.

As a source of reliable information, the Internet must be approached with great caution. As a means with which to gain access to quality commercial sources of validated information, the Internet is unbeatable.

A vision of open source exploitation must not be limited exclusively to electronic sources. Traditional print, hardcopy images and other analog sources continue to provide a wealth of data of continuing relevance to NATO intelligence.

The Open Source Intelligence Cycle

As the range of NATO information needs varies depending upon mission requirements, it is virtually impossible to maintain a viable collection of open source materials that address all information needs instantly. The focus should be on the collection of sources, not information. With knowledge of relevant and reliable sources of open source information, an intelligence staff can quickly devote collection energy and analytical expertise to develop tailored OSINT products to the mission need.

OSINT and the Emerging Future Intelligence Architecture of NATO

OSINT is an essential building block for all intelligence disciplines. Open sources have always played a role in classified intelligence production. In the NATO context, a robust OSINT capability greatly increases the range of information sources available to intelligence staffs to address intelligence needs.

Nations are capable of tasking classified intelligence sources to address intelligence gaps. Lacking organic intelligence collection assets, NATO intelligence staffs are unable to task classified collection. Rather than immediately directed a Request For Information (RFI) to a national intelligence centre, a robust OSINT capability enables intelligence staffs to address many intelligence needs with internal resources.

While unable to replace classified intelligence production, OSINT is able to compliment an all-source intelligence production process with essential support including tip-offs, context, validation and cover for information sanitation.

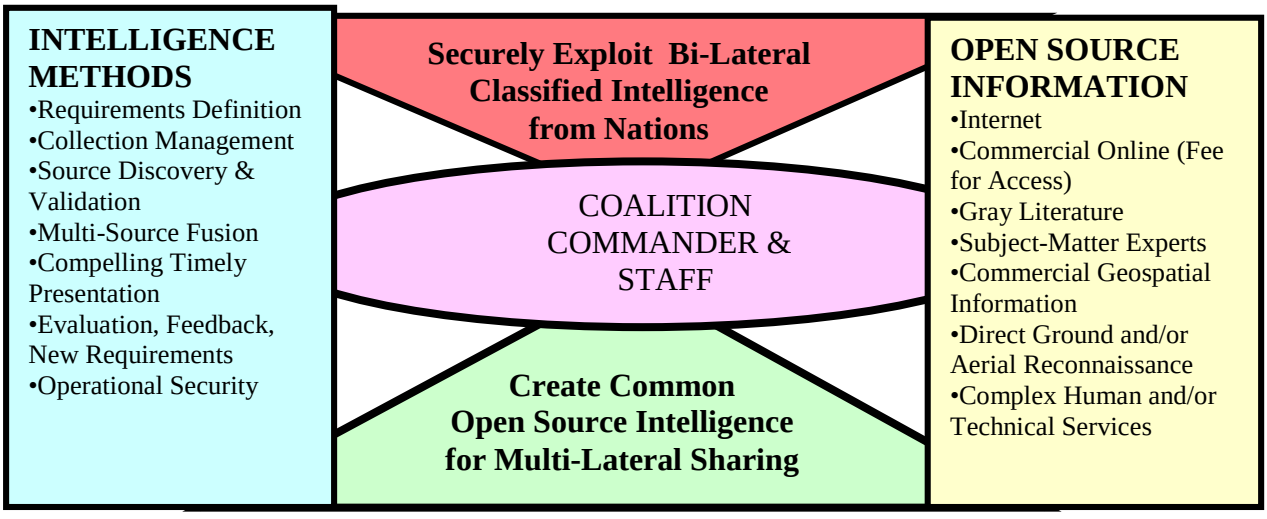
CHAPTER I
OPEN SOURCE INTELLIGENCE AND JOINT OR COALITION OPERATIONS

"OSINT is not a substitute for satellites, spies, or existing organic military and civilian intelligence capabilities. It is, however, a foundation—a very strong foundation—for planning and executing coalition operations across the spectrum from humanitarian assistance to total war. OSINT provides strategic historical and cultural insights; it provides operationally helpful information about infrastructure and current conditions; and it provides tactically vital commercial geospatial information that is not available from national capabilities. In coalition operations, OSINT is both the foundation for civil-military cooperation, and the framework for classified bilateral intelligence-sharing."

Introduction

OSINT is distinct from academic, business or journalistic research in that it represents the application of the proven process of national intelligence to a global diversity of sources, with the intent of producing *tailored* intelligence for the commander. OSINT is also unique, within a coalition operations context, in that it simultaneously provides a multi-lateral foundation for establishing a common view of the shared Area of Operations (AOO), while also providing a context within which a wide-variety of bi-lateral classified intelligence sharing arrangements can be exploited. Figure 1 illustrates these relationships.

Figure 1 - Relationship between Open Source and Classified Information Operations



OSINT is valuable to NATO member nations and to individual Partner nations in that it can be used to provide a common understanding of the AOO across all elements of its military forces and its civilian and non-governmental organization (NGO) counterparts. Elements of the forces not authorized access to the full range of classified information, often including such vital components, as military police, logistics elements, engineers, and the public affairs staff, can be made more effective through the utilization of tailored OSINT. At the same time, external parties with whom coordination is critical, but who are also not authorized access to classified information, can receive tailored OSINT that is helpful to a shared understanding of the AOO and the challenges facing the coalition and all its elements. Figure 2 illustrates this idea.

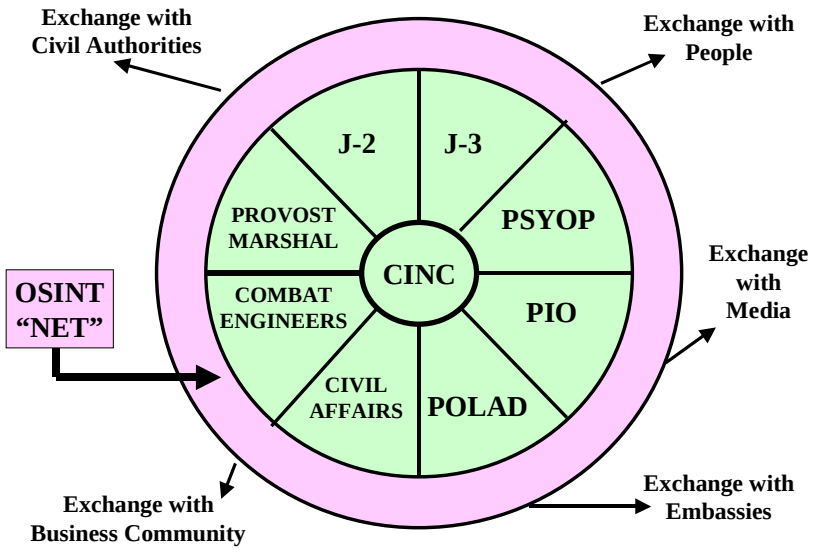


Figure 2 - Utility of OSINT Net for Internal and External Information Exchanges

Definitions

There are four distinct categories of open information and intelligence.

Open Source Data (OSD). Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual.

Open Source Information (OSIF). OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is *generic* information that is usually *widely disseminated*. Newspapers, books, broadcast, and general daily reports are part of the OSIF world.

Open Source Intelligence (OSINT). OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a *select*

audience, generally the commander and their immediate staff, in order to address a *specific* question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and *creates intelligence*.

Validated OSINT (OSINT-V). OSINT-V is information to which a very high degree of certainty can be attributed. It can be produced by an all-source intelligence professional, with access to classified intelligence sources, whether working for a nation or for a coalition staff. It can also come from an assured open source to which no question can be raised concerning its validity (images of an aircraft arriving at an airport that are broadcast over the media).

21st Century Information Operations

OSINT is an essential contextual and foundation element for classified intelligence operations. Overt human sources can help target and validate clandestine human intelligence (HUMINT) sources. Overt broadcast information can be used to better understand covertly collected signals intelligence (SIGINT). Commercial geospatial information, especially wide-area surveillance imagery, can be used to significantly enhance the value of the more narrowly focused covert imagery intelligence (IMINT) capabilities. OSINT can also make contributions to the emerging discipline of Measurements and Signatures Intelligence (MASINT), to Counter-intelligence (CI), and to Operations Security (OPSEC).

OSINT is the major new "force" in 21st Century Information Operations (IO). OSINT is not "new" in that Nations and organizations have always understood the value of legal travelers, direct observation, structured reading, and legal purchases of information services. What *is* new about OSINT is the confluence of three distinct trends: first, the proliferation of the Internet as a tool for disseminating and sharing overt information; second, the consequent and related "information explosion" in which published knowledge is growing exponentially; and third, the collapse of many formerly denied areas.

OSINT is important to coalition commanders and their staffs for another reason: emerging threats, and the lower end of the spectrum of conflict, increasingly demand out-of-area operations and engagement in operations for which classified intelligence support is not readily available. Out of area operations such as humanitarian assistance and disaster relief operations in the countries of Africa or elsewhere along the NATO periphery, are all characterized by complex information needs related to infrastructure, demographics, health, and other matters not traditionally addressed by classified intelligence collection operations.

OSINT is vital to government operations, and especially to coalition operations, for one additional reason: the changing nature of command & control in the 21st Century. In the past, nations and even coalitions relied heavily on a top-down "chain of command" that relied on closed sources to direct generally unilateral actions with short-term time frames. Today, as non-governmental organizations come to the fore and are often the predominant factors in many of the operations that the military must support, the dynamics of both command & control and information have changed.

Within NATO, operations must be planned and executed in a multi-cultural fashion, with bottom-up consensus often being the most effective means of arriving at sustainable decisions. This is particularly true with the vital role played by non-NATO troop contributing nations. Under these circumstances, a common view of the

operating area, formed with the help of validated OSINT is often the most effective means of delivering decision-support.

The remainder of this manual will discuss private sector information offerings, the open source intelligence cycle, and the integration of OSINT into the NATO and prospective PfP coalition operations. OSINT will be a core element of the NATO Future Intelligence Architecture.

Special Note on Operational Security

The most common objection to the use of open sources of information, apart from the general lack of knowledge and funding with which to exploit open sources, relates to Operational Security (OPSEC). This topic is fully discussed within Chapter III. The Open Source Intelligence Cycle makes full provision for OPSEC at every stage, and ample methods exist to conceal the commander's intent, the source of the inquiry, and other sensitive aspects of open source exploitation.

CHAPTER II
PRIVATE SECTOR INFORMATION OFFERINGS

The four pillars to an OSINT strategy are sources, software, services and analysis. The private sector can address all four to some degree. Analysis is the key enabling skill that is essential to the successful integration of OSINT into an all-source intelligence product. While some analysis of open sources can and should be acquired from private sources, those analytical skills necessary to integrate open source derived intelligence must be grown and nurtured within intelligence staffs. Analysis will be discussed further in Chapter III. This chapter is intended to expose the wider audience to the range of OSINT-related products that the private sector are optimized to provide.

SECTION A. SOURCES

Traditional Media Sources

To many, media sources were the only open sources that were familiar prior to the onset of the Internet. These include traditional foreign print and broadcast media, radio and TV as well as the current array of electronically available products. For current intelligence purposes, media sources remain the core capability necessary for an OSINT effort and are available from a variety of providers. Direct wire-service feeds are available. Commercial online premium sources discussed below all provide an array of media sources on a fee for service basis.

While not private sector information providers, the U.S. Foreign Broadcast Information Service (FBIS) and the British Broadcasting Corporation (BBC) Monitoring Service each provide excellent near real-time translation of foreign media sources. In addition, an array of media analysis products supplement the direct listing of foreign broadcasts and provide useful insight into the general character of foreign media reporting on particular issues.

Internet

The Internet has, since 1994, literally exploded on to the world scene and changed forever the manner in which individuals might carry out global research. According to Dr. Vinton Cerf, acknowledged by many to be one of the founders of the Internet, it will grow from 400 million users in November 2000, to an estimated 3.5 billion users by the year 2015.

Apart from this exponential increase in the number of human beings using the Internet, other experts project a double or triple order of magnitude increase in the use of the Internet to connect devices, from geospatial locators in vehicles, to temperature detectors in soda machines, to usage monitors in doorways. The Internet is at the very beginning of its development as a global grid of enormous value to coalition operators, logisticians, and intelligence professionals.

Figure 3 - Internet users by continent (1999)

The Internet has been over-sold in the past. A study by the Community Open Source Program Office (COSPO) within the U.S. Intelligence Community concluded in 1994 that the Internet only contained roughly 450 useful substantive sites, and that 99% of the Internet was not content of intelligence value, but rather pornography, opinion, and advertising. This earlier evaluation of the intelligence potential of the Internet no longer reflects the extensive content that is now available. Some suggest that over 250,000 databases are now available within the "deep web", a great many of which are of potential intelligence value.

While the Internet has grown substantially in value since 1994, the intelligence professional must be very cautious about both over-reliance on the Internet, and about the source bias of materials found there. In general, Internet sources are rarely dated, formatted, paginated, edited, filtered, or stable, even when addressing substantive topics.

The Internet is an "easy out" for operators and other consumers of intelligence. It is an attractive option for commanders and staff in a hurry. If intelligence professionals do not demonstrate that they monitor and exploit the Internet, and/or if intelligence professionals make it too difficult for consumers to obtain usable all-source intelligence, the Internet represents a "threat" to the existing intelligence process. Increasingly, intelligence professionals must act to place information that is widely available on the Internet into its proper context – either confirming its validity or disputing the information based on classified collateral reporting.

In general, the Internet today provides two benefits to the coalition professional: first, as a means of rapidly communicating with counterparts around the world, primarily to exchange unclassified information and professional insights; and second, as a means of rapidly accessing both free and premium (fee paid for access) information sources. However, the Internet also has its dangers. Electronic mail and attached documents comprise a permanent record in cyber-space, and the sender has little control over subsequent dissemination and exploitation.

OSINT Professional Note: A number of advanced search tools are available that complement the variety of search engines that are freely available on the Internet. OSINT managers should remain abreast of developments in the field of Internet tools and integrate appropriate tools, as they become available, into their OSINT process. An example, its basic form available free or in an advanced version at a small cost, is a meta-search engine that combines the best features of multiple search engines, while also permitting subsequent searches for new information (remembering what has already been seen). Download this program from www.copernic.com.

Commercial Online Premium Sources

There are numerous commercial online premium sources, that is, sources that charge either a subscription fee or a usage fee for access to their information. It is essential that every professional understand the availability and the value of commercial online premium sources. They represent decades worth of editorial selection,

authentication, formatting, indexing, abstracting, and presentation management. In general, source material obtained through a commercial online premium service has been created by a reputable commercial enterprise subject to scrutiny and the judgment of the marketplace. In Figure 4, we discuss the three best known to governments and corporations. There are many others, some unique to Europe or Asia. Each professional is urged to consult his or her librarian or his or her OSINT collection manager to gain a better understanding of what their options are for high-quality commercial information relevant to their action responsibilities.

In general, and in part because of the high cost of mistakes or unnecessary retrievals, all commercial online premium services should be searched by those staff with sufficient training on the database and a thorough understanding of its pricing structure. Even commands with flat-fee pricing should be aware that their next contract will be increased in price based on actual usage during the current flat-fee period. Alternatively, an option is to gain access to commercial sources via the services of a professional librarian or commercial information broker. Most professional information brokers, such as those belonging to the Association of Independent Information Brokers (AIIB), specialize in either LEXIS-NEXIS or DIALOG. There are distinct advantages in contracting a searcher who has detailed familiarity with the very arcane search command characteristics of these two services. In the case of Factiva this is less vital but can still make a big difference in both the success of the searchers, and the cost of the searches.

FACTIVA	LEXIS-NEXIS	DIALOG
www.factiva.com	www.lexis-nexis.com	www.dialog.com
Best web-based user interface, easiest means of searching all available publications. Archive of publications varies but typically provides several years worth of historical file. Includes Jane's Information Group material as well as BBC transcripts. Does not include FBIS information.	Two separate channels, one focused on legal sources including public records (primarily in the United States but very helpful in tracing real estate, aircraft, and water craft including international ships), the other focused on news sources but offering archive access, i.e. ability to reach back several years or more on any topic.	A very large collection of various commercial offerings that can be searched "by the file". Especially valuable for access to conference proceedings, academic and policy journals, dissertations, book reviews, and the Social Science Citation Index (SSCI). The latter is ideal for finding and ranking individual experts, to include identification of their official address.
Flat fee or actual cost pricing.	Flat fee, actual cost, or pay as you go credit card pricing.	Flat fee, actual cost, or pay as you go credit card pricing.

Figure 4 - Leading Commercial Online Premium Sources

OSINT Professional Note: Always ask for search results in electronic form, these files can more easily be shared. Copy the results into a Word document. Add pagination. Add a title page and a blank table of contents page. Sort the items into larger categories (e.g. Political, Military, Economic) and label the categories as "Heading 1". Then go through the document label each individual headline as "Heading 2". These headings are choices in the style bar at the upper left that generally says "Normal". Finally, go to the Table of Contents and use the Insert, Index and Tables, Table of Contents choices to insert a table of contents. If desired, use the Replace function to find and make bold all of the original search terms.

Other Forms of Commercial Online Information

There is a vast range of commercial sources available through direct subscription, both on the Internet and in the form of hard copy or CD-ROM publications. Table 1 below identifies just a few sources of common interest to military commanders and their staff. There are many more than those listed here. SACLANT has undertaken to develop and maintain a common NATO inventory of open sources and access points to which RFIs can be directed. This can be found on MCCIS at www.saclant.nato.int/intel. Work continues to progress on a concept of operations for establishing broad NATO access to such sources at the most competitive prices possible.

Source Type or Function	Source Name and URL
Broadcast Monitoring	BBC Monitoring http://news.monitor.bbc.co.uk/
Broadcast Monitoring	FBIS/NTIS World News Connection http://wnc.fedworld.gov/ntis/home.html
Commercial Imagery	Autometric http://www.autometric.com/AUTO/SERVICES/GIS
Current Awareness (Conferences)	British Library Proceedings http://www.bl.uk/services/bsds/dsc/infoserv.html#inside_conf
Current Awareness (Journals)	ISI Current Contents http://www.isinet.com/
Current Awareness (Regional)	Oxford Analytica http://www.oxan.com/
Defense Monitoring	Janes Information Group http://www.janes.com/geopol/geoset.html
Defense Monitoring	Periscope http://www.periscope1.com
Defense Monitoring (NATO)	Orders of Battle Inc. http://orbat.com
Directories of Experts	Gale Research http://www.gale.com/
Foreign Affairs Discussions	Columbia U. Int'l Affairs Online www.ciaonet.org
Foreign Affairs Monitoring	Country Watch.com www.countrywatch.com
Global Risk Monitoring	Political Risk Service (Country Studies) www.prsgroup.com
Maps & Charts	East View Cartographic http://www.cartographic.com

Table 1 - Examples of specialized commercial information

Grey Literature

Grey literature is that information that is both legally and ethically available, but only from specialized channels or through direct local access. It is generally understood as that information whose distribution is not controlled by commercial publishers, and/or that information that is not published, distributed, catalogued or acquired through commercial booksellers and subscription agencies. Grey literature includes working

papers, pre-prints, technical reports and technical standards documents, dissertations, data sets, and commercial imagery. Producers of grey literature include: non-profit and educational organizations; commercial enterprises creating documents for internal use as well as for clients and suppliers; local, state, and national government agencies producing materials for internal use as well as for citizens and vendors, and; a wide variety of informal and formal associations, societies, and clubs. Examples include university yearbooks, yacht club registries, corporate trip reports, and personal notes from public events that are posted to a public bulletin board.

Overt Human Experts and Observers

The ultimate open source is a human expert or human observer with direct experience. In many places of the world, Africa, for example, it is not possible to obtain published information on specific locations or conditions. For many topics, even those with great quantities of published information, it is not possible to find exactly what is needed even when the time and money is available to collect, process, and analyze all available published information. The human expert is often the most efficient and the most inexpensive means of creating new open source intelligence that is responsive to a specific requirement from the commander or his staff.

The identification and interviewing of those with direct on-the-ground experience is also a valuable means of ascertaining "ground truth." It merits comment that official communications from organizations, and most media reporting, tend to rely on second-hand reports. Unless the information is meticulously sourced and from a very trusted source, expert judgment or observation more often than not it will be less reliable than direct human expert judgment or observation.

OSINT Professional Note: There are essentially four ways to get to expert humans. The most effective means is through citation analysis using the *Social Science Citation Index* (SSCI) or the *Science Citation Index* (SCI). These can both be accessed at www.isinet.com/isi. This generally requires a specialist searcher with access to DIALOG for the SSCI or to the Scientific and Technical Network (STN) for the SCI. The second means is through professional associations such as listed in the *International Directory of Associations* published by Gale Research, or as found through a copernic.com search of the Internet. The third means is by doing a Factiva.com search and identifying experts or "talking heads" that have been quoted in the media on that topic. Last, and often the least efficient, is through a labor-intensive series of telephone calls to various known government agencies or official points of contact. As a general rule, it is best to do a comprehensive professional search for international experts with the most current knowledge, rather than relying on the in-house focal points or whomever might be casually known to in-house points of contact.

Commercial Imagery

The commercial imagery industry continues to mature with the launching in recent years of a number of satellites that offer militarily significant capabilities. One-meter

resolution electro-optical imagery available to the private sector is not only possible now but also likely to be *de rigueur* in the future. Table 2 illustrates some of the military applications of 1-m commercial imagery. By 2003, at least eleven private companies expect to have high-resolution commercial remote sensing satellites in orbit. Their products will be available to whoever has a credit card. While this will bring new capabilities to friend and foe alike, commercial imagery provides unique opportunities for NATO as well. Unbridled by security constraints, which limit the use of imagery derived from military satellites, commercial imagery acquired by NATO can be freely distributed within the constraints of copyright agreements with the original provider. This provides a host of options regarding cooperation with broader coalition partners who do not have access to NATO classified information.

Target *(note a)*	**Detection** *(note b)*	**General ID** *(note c)*	**Precise ID** *(note d)*	**Description** *(note e)*	**Technical Analysis**
Troop units	**6.0**	**2.0**	**1.20**	**0.30**	**0.150**
Vehicles	**1.5**	**0.6**	**0.30**	**0.06**	**0.045**
Aircraft	**4.5**	**1.5**	**1.00**	**0.15**	**0.045**
Airfield facilities	**6.0**	**4.5**	**3.00**	**0.30**	**0.150**
Nuclear weapons components	**2.5**	**1.5**	**0.30**	**0.03**	**0.015**
Missile sites (SSM/SAM)	**3.0**	**1.5**	**0.60**	**0.30**	**0.045**
Rockets and artillery	**1.0**	**0.6**	**0.15**	**0.05**	**0.045**
Surface ships	**7.5-15.0**	**4.5**	**0.60**	**0.30**	**0.045**
Surfaced submarines	**7.5-30.0**	**4.5-6.0**	**1.50**	**1.00**	**0.030**
Roads	**6.0-9.0**	**6.0**	**1.80**	**0.60**	**0.400**
Bridges	**6.0**	**4.5**	**1.50**	**1.0**	**0.300**
Communications					
Radar	**3.0**	**1.0**	**0.30**	**0.15**	**0.015**
Radio	**3.0**	**1.5**	**0.30**	**0.15**	**0.015**
Command and control HQs	**3.0**	**1.5**	**1.00**	**0.15**	**0.090**
Supply dumps	**1.5-3.0**	**0.6**	**0.30**	**0.03**	**0.030**
Land minefields	**3.0-9.0**	**6.0**	**1.00**	**0.30**	**--**
Urban areas	**60.0**	**30.0**	**3.00**	**3.00**	**0.750**
Coasts, landing beaches	**15.0-30.0**	**4.5**	**3.00**	**1.50**	**0.150**
Ports and harbors	**30.0**	**15.0**	**6.00**	**3.00**	**0.300**
Railroad yards and shops	**15.0-30.0**	**15.0**	**6.00**	**1.50**	**0.400**
Terrain	**--**	**90.0**	**4.50**	**1.50**	**0.750**

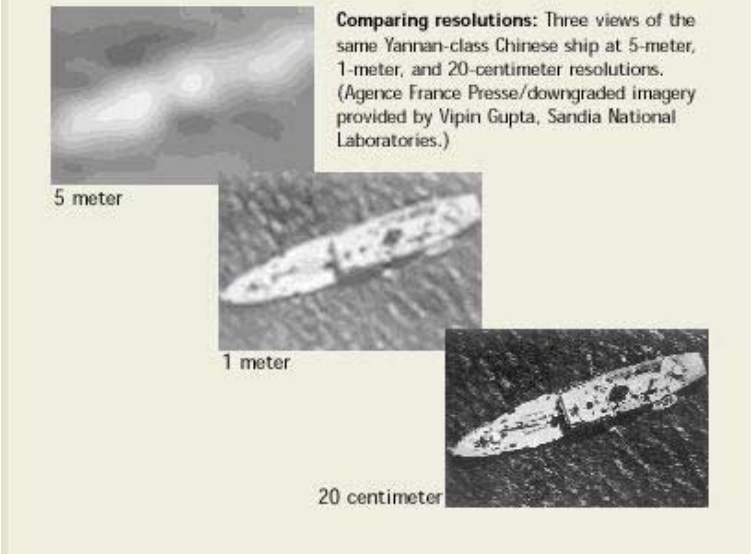
Notes:

a. The table indicates the minimum resolution in meters at which the target can be detected, identified, described, or analyzed. No source specifies which definition of resolution (pixel-size or white-dot) is used, but the table is internally consistent.
b. Detection: location of a class of units, object, or activity of military interest.
c. General identification: determination of general target type.
d. Precise identification: discrimination within a target type of known types.
e. Description: size/dimension, configuration/layout, components construction, equipment count, etc.
f. Technical Analysis: detailed analysis of specific equipment.

Table 2 - Approximate Ground Resolution in Metres for Target Detection, Identification, Description and Analysis

Source: Yahya A. Dehqanzada and Ann M. Florini. *Secrets for Sale: How Commercial Satellite Imagery Will Change the World*. Washington D.C.: Carnegie Endowment for International Peace, 2000.

The individual satellites are currently limited by poor revisit times to specific targets. This factor is mitigated by the growing "virtual constellation" of commercial remote sensing satellites that is comprised of the collective resources of all of the available private companies. The Western European Union (WEU) satellite center has grown its capability through the concept of exploitation of all available commercial resources rather than restricting to merely European sources.



Comparing resolutions: Three views of the same Yannan-class Chinese ship at 5-meter, 1-meter, and 20-centimeter resolutions. (Agence France Presse/downgraded imagery provided by Vipin Gupta, Sandia National Laboratories.)

Figure 5 - Comparative imagery resolutions

In addition to electro-optical sensors, Synthetic Aperture Radar (SAR) imagery capability is improving significantly. SAR imagery relies upon the analysis of a signal transmitted in the microwave part of the electromagnetic spectrum and the interpretation of its return signal. Unlike electro-optical systems, these sensors are not limited to daylight operations. Because they have an active sensor, they can image a target in day or night, in any weather, through clouds and smoke.

While current systems are capable of 8-meter resolution, the next few years will see commercial SAR satellites providing 1-meter resolution. These systems will be able to provide a dependable source of militarily significant commercial imagery to NATO forces as well as to our adversaries.

A number of NATO nations purchase commercial imagery to support their own national imagery requirements. In many cases, these images can be redistributed freely. While NATO commands are able to purchase commercial imagery themselves, national sources of imagery should be consulted, as part of any collection effort, to ensure that commercial imagery needs cannot be addressed through existing sources.

The "virtual constellation" of commercial remote sensing satellites will ultimately be able to provide a target revisit schedule that will increase its reliability as a source of imagery. Until that time, the vast archive of commercial remote sensing images remains a rich source of historical data that can be acquired fast and at low cost. Historical data is optimized for mission planning, mapping and humanitarian support operations when detailed knowledge of infrastructure is essential.

Defining Source Access Requirements (Dangers of Pay-per-View)

It is a relatively easy endeavor to identify private information sources that can support the information needs of an OSINT programme. With the proliferation of restricted and open access Intranets, there are great pressures to place all information acquired onto web-based dissemination systems.

While single copy licenses to information

sources are typically attractively priced, multiple user licenses increase in price. License costs are generally a factor of the number of users that have access to the information. To place information directly onto servers without the knowledge and consent of the information provider is a violation of copyright laws.

An option to reduce costs is to determine the information needs of the organization based on communities of interests. Some information is required by all staff and merits a general site license. Other information is of interest to a more restricted audience. Lloyd's shipping data, for example, may be of general interest to a wider audience but of job specific interest to a select group of analysts. The purchase of a limited site license and the use of restricted access within the Command's Intranet will greatly reduce license costs yet still provide the information in the most effective manner. Finally, ad hoc information requirements may be addressed with the acquisition of single copies of key information sources.

As a general rule, there are few information sources that are required by all members of a staff. Restricting access to some sources will increase the range of open sources that are available for purchase within an organization's OSINT budget. Careful planning and the identification of the logical communities of interest for individual open sources is a reasonable approach to manage scarce resources.

SECTION B. SOFTWARE

Software Hierarchy

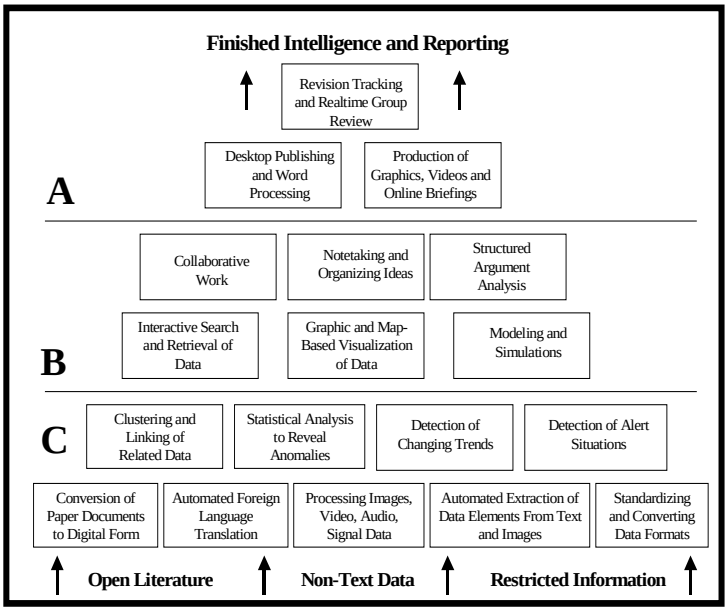


Figure 6 - OSINT Software Hierarchy

Above is an illustration of the eighteen distinct software functionalities that have been identified as being necessary for the optimal processing of open sources of information by any analyst—these would comprise the desktop "toolkit."

Section A functionalities include publishing and production management functionalities. Section B functionalities combine

collaborative work tools with data visualization and manipulation tools with thinking tools: modeling and simulation and structured argument analysis. Section C functionalities combine tools for the automated pre-processing of data once it is digital, and with tools for converting hard copy and multi-lingual or multi-media information into a single digital standard.

Unfortunately, the state of the software industry in general, and of desktop software in particular, is such that today it is not possible to integrate all of these functionalities at an affordable cost. A major obstacle to progress is the existing industry practice of concealing and constantly changing Application Program Interfaces (API). This means that third party software producers desiring to have their offerings work with another major product, must undertake lengthy and often expensive negotiations in order to be shown the proprietary API. Software today is still not "plug and play", and it is unlikely to become fully intergratable "out of the box" until standards of stability and transparency for API are established.

Having said this, it is possible to identify several software packages of some value to the open source intelligence analyst or the action officer working with open source intelligence.

SECTION C. SERVICES

Collection Services

Collection services include online collection (searchers that specialize in Internet, deep web and premium commercial online source exploitation); off-line grey literature or document acquisition; telephone surveys and electoral or other forms of polling; private investigations and human intervention services ("boots on the ground"); and aerial surveillance or reconnaissance services.

Processing Services

Processing services include data conversion from hard-copy or analog to digital, indexing and abstracting of hard-copy or soft-copy textual data or images, interpretation and annotation of imagery or signals, database construction and stuffing, and complex modeling & simulation projects with the best ones including geospatial and time-based visualizations.

When integrated with well-planned open source collection and the right analytical expertise, complex processing services can yield substantial dividends by compressing large amounts of data into manageable tailored products that address specific intelligence requirements.

Analysis & Production Services

A wide variety of commercial and academic organizations offer diverse analysis and production services. As a general rule, the best value is found through the hiring of single individual experts with no overhead, rather than through broad contracts with organizations that then adds a substantial fee for their considerable overhead expenses.

The very best value results when niche collection, niche processing, and niche analysis services can be "mixed and matched" to obtain precisely the desired results. The very worst value comes when an organization is hired because of a convenient contract, they do not have a niche expert, and choose to dedicate an

analyst that does not bring sufficient experience or skill to the task.

Industry leaders can best be identified with reference to citation analysis and familiarity with their product set. This is best accomplished through the identification of other organizations with similar intelligence problems and exchanging information concerning those validated information vendors that they employ. Web-site analysis is another tool, which can be applied to vet the capabilities of a potential information vendor.

Services Examples

Data Conversion	ACS Defense www.acsdefense.com
Database Construction & Stuffing	ORACLE www.oracle.com
Document Acquisition	British Library Document Centre http://www.bl.uk/services/bsds/dsc/
Human Intervention	The Arkin Group www.thearkingroup.com
Imagery Interpretation & Annotation	Boeing Autometric www.autometric.com
Indexing & Abstracting	Access International http://www.accessinn.com/
International Studies Analysis	Monterey Institute of International Studies www.miis.edu
Modeling & Simulation	Boeing Autometric www.autometric.com
Online Collection	Association of Independent Information Professionals www.aiip.org
Open Source Intelligence Portal (meta-service)	Open Source Solutions Inc. www.oss.net
Private Investigation	Intelynx (Geneva) www.intelynx.ch
Scientific & Technical Analysis	CENTRA www.centratechnology.com
Signals Processing	Zeta Associates Incorporated www.zai.com
Telephone Surveys (Primary Research)	Risa Sacks & Associates www.rsacksinfo.com

Table 3 - OSINT Related Services

As a general rule, there are no "portal" companies that serve as honest brokers for helping governments "mix and match" best in class niche providers at the most economical cost.

CHAPTER III
THE OPEN SOURCE INTELLIGENCE CYCLE

SECTION A. OSINT PLANNING AND DIRECTION

Overview

Whether one is going after open source data, information, or intelligence, there is a proven process of intelligence, the intelligence cycle that will yield good value when applied. The open source intelligence process is about discovery, discrimination, distillation, and dissemination—the 4 Ds (Figure 7). This analytical approach is applied to the traditional single source intelligence cycle. A good understanding of the open source intelligence cycle makes it possible to access and harness private sector knowledge using only legal and ethical means, generally at a very low cost in comparison to covert technical or clandestine human collection. Since many requirements that are urgent for the commander and their staff may not qualify for nor be appropriate for secret collection methods, the open source intelligence cycle is in fact *vital* to NATO planning and operations. As will be seen in the following discussion, OSINT is an emerging discipline and the emphasis will often be on informal coordination rather than formal tasking.

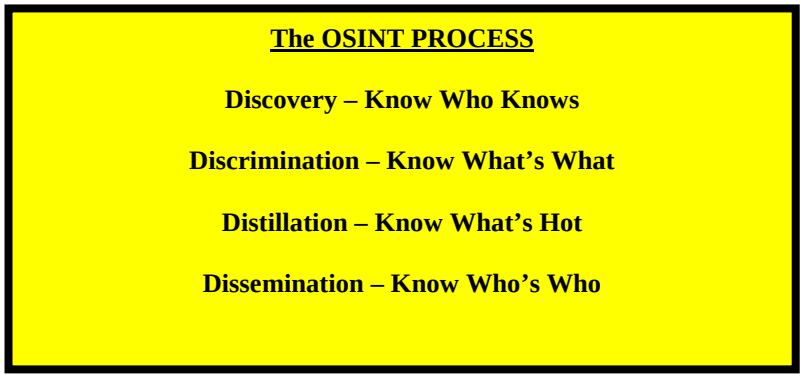


Figure 7 - The OSINT Process

Organizations and Responsibilities

The commander is ultimately responsible for establishing the Essential Elements of Information (EEI) and for applying the resources necessary to satisfy them. Open source intelligence is *not* necessarily the responsibility of, or available from, national-level intelligence organizations. While the intelligence staff typically acts as the staff principal for OSINT activities, other staffs are frequently well placed to both collect open sources and to facilitate the further development of sources on behalf of the Command. The subordinate commanders for Civil Affairs, Public Relations, Military Police, and Combat Engineering may often be the best channels for seeking out OSINT, and can comprise an informal advisory council to the commander.

OSINT sources include, but are not restricted to:

- **National-Level Intelligence Organizations**. Although they are not responsible for satisfying the commander's needs for OSINT, national-level intelligence organizations may have relevant open source information that can be provided. Some countries, such as The Netherlands, United Kingdom, Denmark and Norway, are exceptionally competent in this area and have fully integrated OSINT into their all-source collection and production environments. Others may have selected units that can be called upon, but have not yet mastered this discipline.

- **Diplomatic Missions**. The established diplomatic missions of the various member nations are often the best source of OSINT, at little cost, if they are approached by one of their nationals acting in an official capacity on behalf of the commander. Such missions are under no direct obligation to respond, but informal coordination may yield good results.

- **Chambers of Commerce**. Many of the member nations have Chambers of Commerce and these often have established small communities that bring the general managers and key business executives from their national firms in any given country together. On an informal basis, with clear disclosure of the commander's interest, useful OSINT may be acquired. This is particularly true in deployed areas.

- **Non-Governmental Organizations**. The International Committee of the Red Cross (ICRC), Doctors Without Borders, and the many elements of the United Nations as well as the many international relief and charity organizations, have deep direct knowledge that can be drawn upon through informal coordination.

- **Religious Organizations**. Many Non-Article 5 Operations have very substantial human mass migration and ethnic conflict aspects as witnessed during Operation Allied Force. These issues are often best understood by religious organizations. Organizations such as The Papal Nuncio and the local Opus Dei, the B'nai Brith, the Islamic World Foundation, and other equivalent religious organizations are an essential source of overt information and expert perceptions

Requirements Definition

The greatest challenge for the commander will be the establishment and maintenance of a rigorous and disciplined process for defining the requirements to be addressed through open sources. The common attitudes of "tell me everything about everything" or "if I have to tell you what I need to know you are not doing your job" represent unworkable direction.

Commanders and their staff must carefully evaluate the specific information needs in the context of their concerns and their plans and intentions, and they must articulate, in the narrowest possible way, precisely what they want to know and why. The commander's operational intent is as vital to the intelligence professional as it is to the operations professional. Only by understanding the context and direction of the commander's requirements, can a truly focused and flexible collection effort be undertaken.

OSINT is the most fundamental and fastest means of satisfying basic informational

needs, including needs for historical background, current context and general geospatial information. Each commander should distinguish between their tailored intelligence requirements in support of their future planning and the basic information requirements that will permit operational and logistics and other special staff planning (e.g. Civil Affairs) to go forward. OSINT is highly relevant to both kinds of intelligence support.

Evaluation and Feedback

Planning and direction is a continuous process. The commander and their staff must digest, evaluate, *and provide feedback on* all received intelligence, whether open or classified. As open source intelligence is received and reviewed, it must be shared with staff principals and subordinate commanders, evaluated, and the results of the evaluation passed directly to the staff element responsible for coordinating OSINT support to the commander.

SECTION B. COLLECTION

Overview

The heart of intelligence collection is research – it is the matching of validated intelligence requirements to available sources with the aim of producing a product that answers a valid need. Once an intelligence need has been identified, open sources should be reviewed by intelligence staffs to determine if that intelligence need can be satisfied through those resources organic to the intelligence staffs, those resources that the staff can access, if an RFI to nations is required, or if a combination of these approaches is required.

Collection requires the translation of an intelligence need into an intelligence requirement – an action plan to answer that need. A collection strategy is developed to tap available sources. Optimal sources are selected and the information is collected. This generic collection approach is equally applicable to classified sources as it is to open sources.

In the NATO context, OSINT is a contributing source to an all-source intelligence effort. Open sources are used to compliment the existing classified intelligence and can be collected on a specific area. OSINT-derived products are created to answer a specific intelligence need to which open sources are best optimized. While RFIs from intelligence users typically generate collection efforts, Table 4 illustrates the three types of producer generated intelligence collection and production requirements.

These three categories outline the way in which an internally directed OSINT

Analyst-driven	**Based on knowledge of customer and issues**
Events-driven	**In response to time-sensitive relevant events**
Scheduled	**Periodic activities to document and update target status**

Table 4: Types of Producer-Generated Intelligence Collection and Production Requirements

Source: Arthur S. Hulnick. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." Intelligence and National Security, Vol. 1,No. 2, (May 1986)

collection strategy should be developed. Only those products that support the intelligence staff's mission should be produced. The range of open information that is available both freely and commercially will swamp the analytical capacity of any intelligence staff regardless of size. Therefore, effective management must include the avoidance of production without a specific purpose. While not advocating a "make work" approach to intelligence, producer-generated collection builds skills, evaluates sources and increases capabilities necessary to address future RFIs and production requirements.

An analyst is often best placed to determine what product is required to address the past needs of the intelligence user. Proactive collection and management to make effective use of emerging information should be encouraged. This could include the tailoring of a newly available public report that addresses an established intelligence need into a format of use to an intelligence user.

Rapidly changing events can drive the production of new products. A military coup or an environmental crisis could presage increased NATO interest in an area of non-traditional interest. In the absence of national intelligence production shared with NATO, open source collection may be the best means with which to begin to build an intelligence picture for the command.

Less dramatic changes to the international environment may also require open source collection. Seasonal changes in a particular region may lead to population migration. These periods are known well in advance and lend themselves to scheduled production of necessary intelligence products.

Chapter II reviewed private sector information offerings. Chapter III focuses on the methods to be applied by any NATO unit to exploit those offerings, while not recommending any specific source, software, or service. What is important is that every NATO unit is conscious of the overall process, the alternative means for obtaining and exploiting OSINT, and the value of OSINT as part of the all-source intelligence cycle. Figure 8 below is provided a high-level view of the elements of the OSINT collection process.

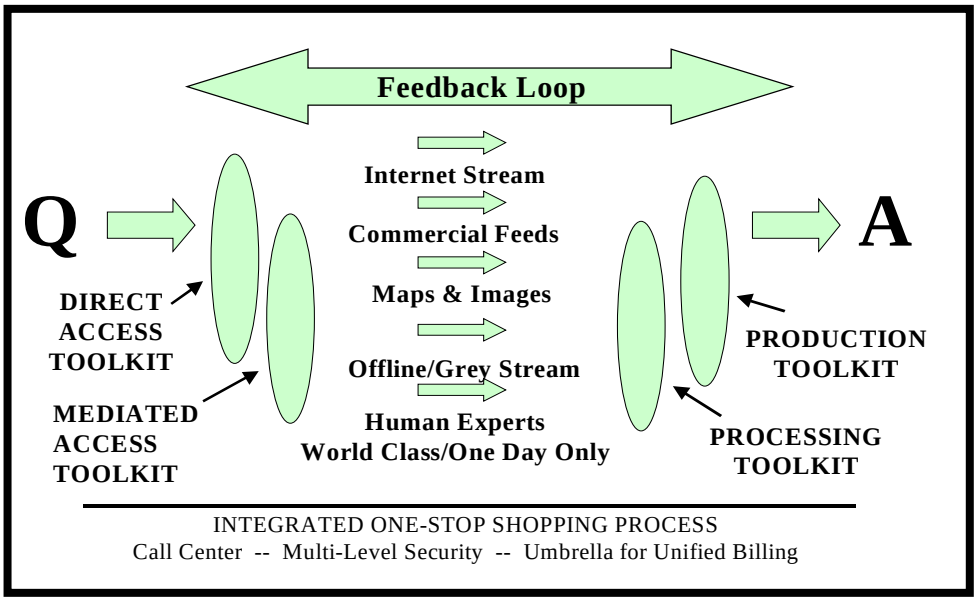


Figure 8 - OSINT Collection Process

Knowing Who Knows

During periods of stability as well as crisis, it is incumbent upon intelligence staffs to establish and nurture sources that will help satisfy information requirements. It is vital that the OSINT professional, known in some governments as Open Source Officers (OSO), focuses initially on "knowing who knows" – the ability to rapidly identify subject matter experts on topics of direct relevance to the commander's mission and to seek information from them.

An approach favoured by some is the concept of collecting sources not information. While the array of available open sources is staggering, the ability to focus collection quickly on an emerging issue of intelligence interest is the key capability. Rather than having a stale open source product to draw upon, the ability to rapidly direct collection on an issue, identify the leading experts on the field and either draw upon their most recent work or contact them directly is the most effective use of an OSINT capability.

Therefore, a standing collection priority should include a preliminary inventory of subject-matter experts (SME) within the parent commands and its subordinate, adjacent, and higher commands, but should then extend further, throughout the parent government and into the national private sector. The business community with its international chambers of commerce, the academic community with its various professional associations, and the non-governmental organizations including the peace institutes resident in many countries, are all vital points of reference.

The command OSO is, in essence, an information attaché to each of these elements, and must always act with the highest standards of overt decorum and propriety. This must include a firm grasp of both the private sector's rights and obligations with respect to copyright and the protection of intellectual property, and NATO's concerns with regard to OPSEC.

Collection Discipline

There is no faster way for an OSO to lose his commander's respect than to try to do too much, and end up taking too long to produce simple answers. Time management, and a very disciplined approach to the art and science of OSINT collection, is the key to every success.

The ever-increasing array of open sources provides a rich environment for unbridled research. OSINT managers must ensure that their staffs are aware of the degree of detail required for each OSINT product being prepared. The Internet and commercial premium online sources are seductive to the analyst. Within any OSINT effort, time spent in collection is always at the expense of analysis. The desire to continue with the

OSINT Professional Note: A recommended timetable for a standard OSINT collection and analysis task is provided below:

15 Minutes	Requirements Definition. Ensure an understanding of commander's intent.
30 Minutes	Internet Collection. Use search tools, rapidly identify top ten sites and review.
15 Minutes	Internet Table. Create Internet Table for future use and for customer's reference.
60 Minutes	Commercial Collection. Use fee sources, identify top 20 items for exploitation.
60 Minutes	Analysis. Read, understand, evaluate, and structure collected information.
60 Minutes	Production. Carefully create an analytical summary, table of contents, and slides.
4 Hours	Total time required to create any OSINT report using only internal resources.

collection and acquisition of open sources at the expense of their evaluation and presentation as an analytical product reduces the effectiveness of the OSINT contribution to the all-source effort. In few other fields is the mantra that "perfection is the enemy of good enough" more appropriate than it is for open source collection. Collection efforts can be reduced if time spent in the evaluation of the reliability and objectivity of specific open sources does not have to be replicated each time an analyst begins a project. OSINT managers should ensure that their staff maintains a dynamic compilation of the open sources that they exploit for specific issues. This reference aid will serve as the starting point for subsequent analytical tasks.

Collection Issues

There are several collection issues that always surface whenever commanders and staff first consider OSINT as a structured discipline. These include OPSEC, Copyright Compliance, Foreign Language Shortfalls, and External Networking.

Operations Security

- OPSEC is easily achievable in the OSINT environment through two measures: first, the concealment of the origin of the search through the use of trusted intermediaries; and second, the utilization of normal commercial Non-Disclosure Agreements (NDA) when necessary to protect direct discussions of a commander's concerns and intentions.

- In general, most OSINT inquiries will be amply protected by existing processes, but when appropriate, a trusted local national with information broker skills can be hired (or a Reservist utilized) to distance the inquiry from the command. It is a misconception to believe that any discussion with OSINT providers must be itself open.

- The private sector is accustomed to protecting proprietary and commercially confidential discussions. A standard private sector NDA is just as a good as a government secrecy agreement, with the added advantage that the private sector partner has a financial motivation for honoring the NDA—they want more business and discretion is part of what they are selling.

Copyright Compliance.

- In the past, many governments have felt that copyright compliance did not apply to their official needs, and some governments have resorted to the classification of open source information as a means of concealing their routine violation of private sector intellectual property rights

- It is now essential for all governments, and for all NATO elements, to learn how to properly comply with applicable copyright provisions. This is important for two reasons:

  - To maintain the highest standards of legal and ethical behavior among all NATO elements;

  - More often than not, OSINT must be shared with external private sector parties (e.g. humanitarian assistance organizations) or used as a means of exchange (pooling information on Kosovo, for example). Thus copyright compliance is a vital means of maintain future *flexibility* in the exploitation of the OSINT available.

Foreign Language Shortfalls.

- Despite the multi-cultural and multi-lingual nature of the NATO alliance, many out-of-area contingencies require

foreign language skills that are not readily available with the NATO force, or that can be identified quickly and provided with security clearances.

- Over time it is vital that each commander identifies foreign language skills as well as shortfalls and that these be consolidated and evaluated as part of the larger NATO Future Intelligence Architecture plan.

- Understanding international terrorism, insurgency, and violent internal political opposition movements, to take one example, requires competency in a number of foreign languages to include: Arabic, Catelan, Danish, Dari, Dutch, English, Farsi, Finnish, French, German, Indonesian, Irish, Italian, Japanese, Korean, Kurdish, Kurmanji, Norwegian, Pashto, Polish, Portuguese, Russian, Serbian, Spanish, Swedish, Tamil, Turkish and Urdu.

- Many of the required capabilities are within the competence of national intelligence organizations but these capabilities are unlikely to be made available to NATO commands for the exploitation of OSINT.

External Networking.

- There are four obstacles to external networking relevant to NATO competency in OSINT.

- First, there is a lack of knowledge about who the real experts are on various regional and topical issues.

- Second, there is a fear of revealing the question as an official inquiry—in some countries; there are even prohibitions against direct contacts between intelligence personnel and private sector experts.

- Third, there is the lack of funding for compensating subject-matter-experts—everything must be done on a barter or exchange of favors or information basis.

- Fourth and finally, the existing command & control, communications, computing, and intelligence (C^4I) architectures tend to prohibit routine access to the Internet, and often make it difficult if not impossible to migrate unclassified information from the Internet into classified databases.

All of these obstacles can be overcome. A major outcome of the new NATO OSINT initiative will be the definition and resolution of each of these obstacles.

Nuances of Open Source Collection

The Internet, although it will never be a completely trustworthy source for information, has become the *de facto* C^4I backbone for everyone other than the military. It is essential that our intelligence, operations and logistics staffs develop new doctrine and new methods for fully exploiting the data sources and the human experts that are easily accessible through this medium. As NATO deals with more and more non-traditional threats and more and more out-of-area as well as civil stability scenarios, OSINT will become a much more important element of the all-source intelligence solution. It is vital that every NATO commander and relevant staff member begin now to understand and plan for their OSINT needs.

Training in open source exploitation is relevant not only to the intelligence professionals, but also to all relevant staff

members who need access to open sources of information. OSINT is not the exclusive purview of the intelligence profession. The intelligence professionals should be available to reinforce the commander and their staff, but as a general rule, if a staff principal can answer his own information requirement exclusively through those open sources available to him, then that staff principal that should manage his own collection effort.

Intelligence staffs should enable all staff elements to access relevant open sources as directly as possible. Intelligence staffs should serve to facilitate the flow of OSINT and open source material while providing source evaluation and guidance. Applying this process will enable many potential RFIs to be self-satisfied and thus not submitted. A robust OSINT programme can reduce the number of unnecessary RFIs that bog-down the all-source intelligence staff with information requests that can otherwise be satisfied.

While each commander will have their preferred means of managing OSINT, what is required is that they have a formal point of contact for OSINT matters, an established process, and that they ensure that OSINT is fully integrated into every aspect of their command & staff operations.

The Internet, despite its current and projected growth, is primarily a vehicle for open collaboration, rather than a repository of knowledge. Commercial online sources such as Factiva, DIALOG, LEXIS-NEXIS, STN and Questel-Orbit have huge repositories of information that have been professional selected, evaluated, indexed, abstracted, structured, and made available in a very stable format with authoritative sourcing, formatting, and dating.

In many cases, the information provided through these services have been “peer reviewed” – an exhaustive evaluation process by established leaders in the field of study to ensure the accuracy of the information and the rigor of the research. The Internet is not a substitute for premium fee-for-service commercial online databases, and it is vital that no NATO element falls prey to this illusion.

Each commercial service, as discussed briefly in Chapter II, has its own strengths and weaknesses. A robust OSINT capability should include the understanding of and the means to exploit each service accordingly. Some are best for current news, others for legal records, and others for access to conference proceedings and dissertations.

According to some OSINT experts, only a fraction of known knowledge is available online, either through the Internet or through the commercial online databases. Grey literature, the limited edition publications that are not available through normal commercial channels, comprises a vital "middle ground" between online knowledge and human expertise capable of creating new knowledge in real time. Therefore the NATO OSINT process includes the inventory and evaluation of grey literature sources, and the development of a strategy, a budget, and a process for assuring that grey literature sources are fully integrated into the NATO future intelligence architecture.

Finally, there is the human element. As OSINT doctrine is developed, it would be helpful to think of three distinct forms of overt HUMINT support to NATO. First and foremost are internal subject-matter-experts. These are scattered across commands and within various elements of the member nations’ governments. Second are the private sector experts who have achieved a favorable reputation based on their proven record of accomplishments and publications. Thirdly, there are "local knowledge" experts, including legal travelers and local residents that are rarely exploited by resident defense attachés for lack of time or funding with which to reimburse individuals for their time and expense.

New means must be found for defining

which local knowledge and local observation is needed, and for combining direct observation by qualified NATO personnel, with out-sourced overt collection and production.

SECTION C. PROCESSING AND EXPLOITATION

Overview

After the vital role played during the collection portion of the intelligence cycle, when "knowing who knows" and being able to "mix and match" niche providers of varying pieces of the OSINT solution is essential, it is in the processing and exploitation portion of the cycle that the OSO really makes a mark.

Open sources, just like clandestine or covert sources, require the application of human judgment in order to sort out the important from the unimportant, the timely from the dated, the relevant from the irrelevant, the trusted from the untrusted. As so much of OSINT is *not* in digital form, hands-on human translation and evaluation are the most important part of processing and exploitation.

Without a dedicated set of automation tools to facilitate the processing of open source information, OSINT production will continue to be reliant upon *ad hoc* software solutions and rigorous analytical effort.

Analysis

When working from open sources, there is considerable danger for the analyst to be susceptible to unwanted biases and deception from open source authors. While it is never wise, nor an acceptable practice, to attribute as fact intelligence solely because it was received from a national intelligence agency, in those cases, the analyst is able to make certain judgments regarding how that agency managed its information prior to releasing its report. This is not always true for open sources. It is essential that the analyst remain mindful of and determine the origin of the information that has been gathered and the degree of trust that can be assigned to it. Appendix C provides a list of some common misperceptions and biases.

In the production of OSINT reports, it is crucial that the reader be aware of what is known and what is being speculated about. The analyst should always be careful to distinguish between information and fact. If the original source material is not provided

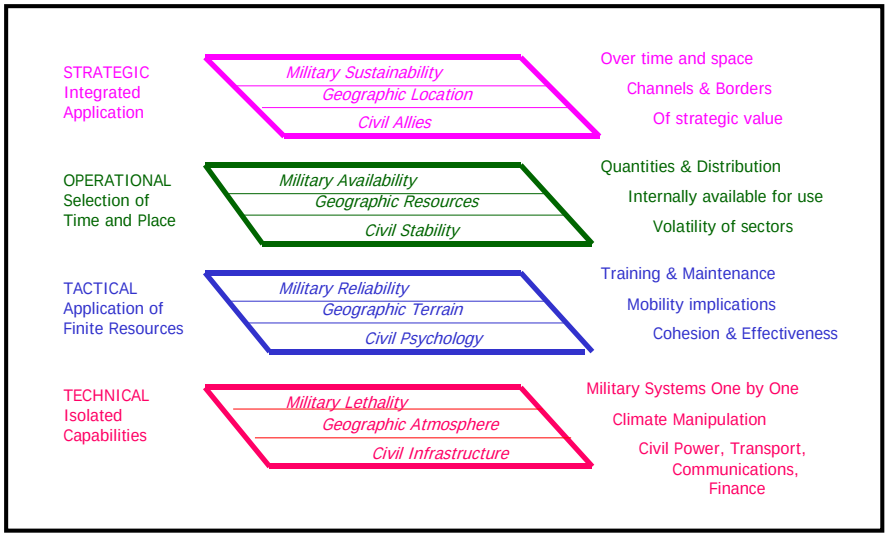


Figure 9 - Levels of Analysis Model

in full text, it is important to make reference to it and provide an assessment of the source's credibility.

If at all possible, the original sourcing information should never be separated from the open source reporting. A complete description of where the open source information was acquired, the identification of the source, the timing of both the production of the open source information and the timing of its acquisition—these all comprise fully half the value of an OSINT product. Without the sourcing pedigree, the open source substance must be considered suspect and of minimal value to the all-source intelligence analysts or the operations or policy consumers being supported.

It is also helpful when processing open source (or classified) information manually to have in mind a clear model of analysis that distinguishes between military, civil, and geographic information, and also between the levels of analysis—strategic, operational, tactical, and technical—for the threat *changes* depending on the level of analysis. This also helps the analyst to recognize gaps in their collected information, and the relationship between different types of information. One such model is provided in Figure 10 above for illustrative purposes.

Web Site Authentication and Source Analysis

Content on the Internet continues to grow at logarithmic rates. The Internet has become an essential enabling element for commerce. It is also facilitating other forms of human interaction across borders which two decades ago were unimaginable. The intelligence value of information found on the Internet is extremely variable. The dangers of creating misleading analysis through the bleeding of unevaluated biased information into the all-source intelligence picture are ever present. Therefore, the OSINT analyst must take steps with each open source to evaluate its reliability. The standard criteria for evaluation of web-sites are as follows:

Accuracy.

- Is the information that is provided consistently accurate based on other sources? The OSINT analyst is able to compare information provided from the web-site with validated all-source intelligence. Benchmarking open sources against validated all-source intelligence assists in assessing the likely accuracy of other information contained on the web-site to be used to address intelligence gaps.

Credibility & Authority.

- Does the web-site clearly identify itself? Is there merely an E-mail address or a full name, address and telephone number. *Sam Spade* (www.samspade.org) is a web service that provides various online tools to validate a web-site. These include diggers that trace routes used by the web-site. (See Web-site Analysis Guide on the following page).

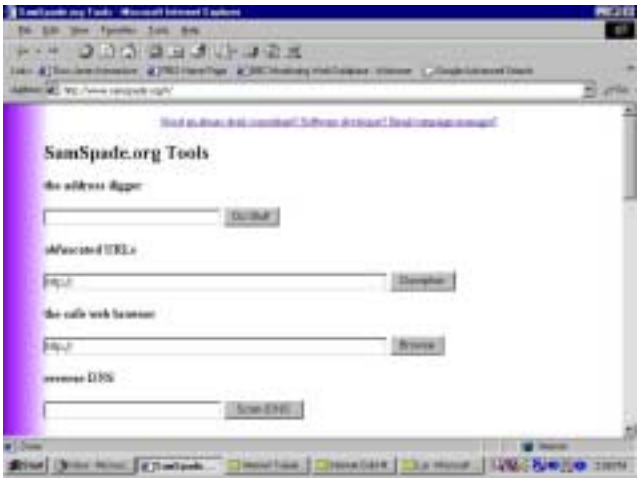


Figure 10 - Web analysis tools

- Does the web-site demonstrate a degree of influence? Do other media cite that web-site in their reporting? Has the web-site been attacked electronically or in official government statements?

- The use of free web-hosts such as Geocities.com or Cybercafe.com often suggest limited financial support for the web-site and a lack of authority in its message.

- Hit-meters/Counters that note the number of times the web-site has been visited can also provide some limited indication as to the influence of the web-site. Thought these can be misleading and should only be used as an element of an assessment of a site's authority.

Currency.

- Does the web-site provide information that is timely or are its pages dated? Some dated information can still be relevant for less dynamic topics (e.g. trade statistics) but may be misleading in tracking current events (e.g. presence of insurgent activity).

Objectivity.

- Does the web-site correspond to a known advocacy group? Does the site represent individuals or an organization? Does that site claim to speak for the organization? Is that site the main web-site or a satellite web-site that represents only a sub-element of the organization.

- To whom does the web-site link? Many sites provide a list of relevant links. These attempt to direct visitors to a community of interests that share similar interests or views. An evaluation of those links can further illuminate the views of the web-site authors.

Relevancy.

- Is the information contained on the web-site relevant to the question at hand? Many web-sites provide information related to a particular topic but do little to add to the understanding of the issue. Information provided can often be interesting but not relevant to the OSINT analyst.

WEB SITE EVALUATION CHECKLIST

Each Internet Website of potential intelligence value must be evaluated as to its suitability for intelligence exploitation *before* it is cited in OSINT reports or used as collateral information in classified reporting. The essential questions remain: who, what, where, when and why?

1. WHO? Examine the URL first. In the page scan for names, and "about" links.

What type of domain is it? (.com / .org / .edu / .gov / .mil / country code) – Is this appropriate for the material presented?
Might it be a personal page? (use of ~ in URL often suggests this)

Who wrote it? **Look for e-mail contact.**
Credentials? **Search on author's name.**
Check source code as webpage's author is often embedded in the code.

Who is the owner of the host server? **Use WHOIS and DNS LOOKUP tools at www.samspade.org to determine the registered owner of the website and evaluate this information. Does this match earlier information gathered?**

What do others say? **Search to see if others cite the author or the web-site.**
Who links to it? **In Google or AltaVista, enter the search string (*link:webaddress)* to find who links to the site. Evaluate the community of interests.**

Opinions of it? What do others think of this website?
Found in any reliable directories? **Determine if the website is contained within reliable web directories or web portals for the topic.**

2. WHAT?

Is the material presented authentic, with sources and dates?
Is data unaltered from its original source?
Note: Little value can be attached to information that is either undated or unsourced.

3. WHERE?

Where does the information originate? **Use www.samspade.org to conduct a TRACEROUTE search. TRACEROUTE will determine the path between your computer and the server hosting the information.**
Is the server located where the author purports to reside? Why or why not?

4. WHEN?

How current is the information provided? **Look for a last updated statement or dates on references.**
How often is the information maintained? Should it contain more recent information?

5. WHY?

What's the page's aim, intent?
Why was it created?
Who sponsor's the page? **Look for an "About us" entry.**

Source: Developed from material created by Joe Barker and maintained on server: www.lib.berkeley.edu.

SECTION D. SEARCHING ANONYMOUSLY ON THE WEB

Overview

While much of the OSINT cycle can be conducted openly, a robust OSINT programme should include a capability to work anonymously on the Internet. Despite the fact that all information on the web is freely available to anyone with a PC and an Internet connection, there are security dangers in searching for it.

All Internet traffic is subject to monitoring at virtually any point by elements external to your organization. It would be of little surprise that NATO was interested in insurgencies in the Balkans and Internet searches on this topic would seem natural from Alliance web addresses. Specific searches on individual leaders of insurgent groups would reveal a heightened interest and potentially reveal intentions. This sort of activity should be protected.

Being anonymous on the web may not necessarily involve deception. It is quite possible to surf the web without openly identifying your identity, purpose or intentions. This is simply a case of "I won't tell you unless you ask."

Before you even start surfing anonymously make sure you don't leave your Internet connection open to attack. You may take all the precautions necessary to hide your intentions and identity whilst surfing, but, without precautions, all the sites that you have visited and all the information you have downloaded is stored on your PC is available via your open connection, then you are vulnerable.

There is an argument for the use a firewall to stop hackers at the front door, but remember that there hasn't been a firewall yet that wasn't eventually cracked. The very expensive firewalls do a good job but it is

Elementary steps to create and maintain an anonymous WEB-Presence

Disable anything that records your activity.

If using MS Internet Explorer:

- **Turn off the cookies**
- **Clean out the history folders, and**
- **Routinely remove cached files.**

Use removable storage media to save any downloaded files to.

Only use your Internet PC for surfing. Do not use the word processor for business or personal letters.

Make sure all your connection details are anonymous.

Ensure the set up of your system is as standard as possible.

Figure 11 - Maintaining an anonymous presence

unlikely that you would want to spend so much money for a simple Internet connection. Besides if you wanted to remain anonymous on the Internet an expensive firewall is not the way to do it. It would highlight the fact that you had something to hide. The same argument applies to the cheaper firewalls. Because they are cheap they are also vulnerable. Hackers know how to get in and often see areas with firewalls as a challenge. One of the best means of security is to remain anonymous and look just like everyone else. By doing this, if a hacker chooses to attack your Internet connection whilst you are online, they would find nothing. The hacker would probably then get bored and never bother you again.

Leaving a Footprint

When you surf the Internet you cannot fail to leave a footprint. A footprint is an electronic signature that identifies you as a unique identity on the Internet during your current session. Most Internet Service Providers (ISPs) now issue a new signature to you each time you log on to surf. But whilst you are surfing during a session after log on, every site you visit retains your electronic signature. If you are trying to find information on a sensitive subject it is possible to carry out an analysis of the sites you visit and the subjects you are searching for. It would be sensible to log off and on again a number of times during a sensitive search.

Although an ISP may provide you with a new signature, part of that signature will identify the ISP. If your organization is large and has its own ISP this will identify your organization. It is always better to go through a civilian ISP whenever possible.

It is possible to use a number of different ISPs. These days there are a huge number of free ISPs available. Each country has its own list of free ISPs and details of these can be obtained via the Internet. It is possible to hide the country from which you are searching from by dialing up an ISP in another country and beginning your search from there. It is almost impossible for a hacker to identify which country your call originated from because Telecoms companies take their personal privacy obligations very seriously.

There is one thing that may identify your country of origin and that is the date and time of your search. When you surf, the date and time of your PC is stamped on the search as part of the electronic signature. If this does not match your ISP time it may indicate that you are trying to hide something, so make sure your PCs time is set to the time zone of the country of the ISP you are using.

Traffic analysis

Every web site has the capability to log the number of visitors to its site and the electronic signature of the visitor. Whilst you may be able to hide your identity, you cannot hide the fact that you have visited the site. If the number of visitors to a significant site increases dramatically then this may be an indicator that there is new or renewed interest in the subject of the site. Such a site may be set up deliberately to identify interest, for example an obscure terrorist related site.

The way to combat this is to ensure that trained personnel, in a central location do all sensitive searches. This will ensure that searches are done quickly and without repetition. The security education of all personnel who have access to the Internet is also a very important factor.

Contact with Others

There may be occasions when you may want to communicate with others to solicit information. In most cases it is beneficial to explain who you are and ask for help or information. There may be other occasions when you may not want others to know exactly who you are or whom you work for. The reasons for this must be decided on a case-by-case basis. It is reasonably easy to create an anonymous persona on the web but the following points should be noted.

It is better to employ discretion rather than deception when soliciting information on the web. This will be less publicly embarrassing later and will make an explanation of your action more reasonable.

An anonymous persona should only be used for occasional requests for information. Any development of a relationship using the Internet should be discouraged. This is the field of other specialists and without proper control can lead to embarrassment.

SECTION E. PRODUCTION

Overview

The four main elements of OSINT production are listed in Figure 12. As

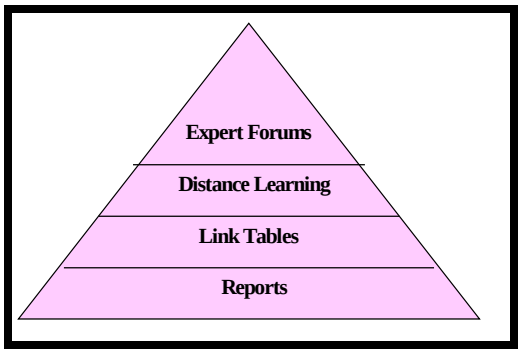


Figure 12 - OSINT Production Elements

opposed to other intelligence disciplines, OSINT relies upon outward engagement beyond the institutional confines of the intelligence staffs. Engagement is essential to the successful exploitation of open sources. This requires knowledge and understanding of information outside of intelligence channels in order to locate and exploit the best sources of information relevant to an intelligence problem and engage them in a meaningful exchange.

OSINT's four production elements will be explained within this section. While the degree of complexity will vary depending upon the intelligence requirement, those four elements will all remain applicable.

A major difference between the OSINT process and the traditional all-source intelligence process exists in how "reports" are treated. In the traditional classified intelligence process, reports are the end of the process—in the OSINT process; they are the beginning, one of four key elements in the *interactive* and *consumer-oriented* process of OSINT support.

Reports

In Chapter One, a distinction was drawn between OSIF, data that has been collated together and is of generic interest, and usually broadcast or widely disseminated and OSINT, information that has been deliberated discovered, discriminated, distilled, and disseminated to a specific consumer in order to answer a specific intelligence need.

NATO OSINT specialists will have occasion to do both kinds, but must be very clear in their own mind, when doing a report, as to whether it is an information report for general broadcast, or an intelligence report for a specific operational purpose.

A report should have an analytical summary. This is value-added expertise from a trained NATO professional who has first screened and integrated multiple elements into an underlying framework, and then devised an executive summary that can stand on its own.

Generally a Report, e.g. a report on Kosovo, will have more than one section, for instance, sections on political, military, insurgents, health, police, and external assistance. Each section should in turn have a short summary, no more than a paragraph in length. The section summaries can be used to create the overall report summary, but should be further distilled and not simply strung together.

Within each section (or linked to each section summary if done in a web-based format) should be between one and five key items of raw information—whether a transcript from a news conference, or a wire service release, or a commercial image, or an extract from a foreign military map.

A major difference between OSINT and other clandestine or covert sources is that OSINT strives to provide concurrently both analytical value and direct access to raw materials. OSINT sources rarely require protection. Text-based products can be stored and disseminated easily by electronic means.

By providing the consumer (the commander, the operator, the logistician, or the all-source intelligence analyst) with direct convenient access to the best of the raw materials, the OSINT analyst is enabling the consumer to dig deeper if they chose to while satisfying the initial RFI.

Reports should always show, on the first page, the date and hour at which collection (not production) was cut off, and the time period in days and/or hours that the report covers. Reports can be organized by source (Internet, Commercial Online, Grey Literature, and Experts) or by topic. They should always identify the author and if appropriate the reviewer of the Report, and provide complete contact information so that readers may quickly ask follow-up questions of the originator.

COUNTRY (e.g. Sri Lanka)

TOPIC (e.g. Economy)

DATE OF INFORMATION (e.g. 26 March 2001, 1500EST)

ANALYTICAL SUMMARY (new value-added analytic summary)

RAW INFORMATION 1 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 2 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 3 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 4 (best of 20 read sources from 200 screened sources)
RAW INFORMATION 5 (best of 20 read sources from 200 screened sources)

Figure 13 - Representative report structure

Link Tables

Internet search engines, even recommended meta-search engines, have severe limitations. By some accounts, any one search engine will cover only 10-15% of the visible web, and even all the search engines working together will overlook what is known as the "deep web." The deep web consists of complex sites with many levels, many free and some by subscription, where search engines are simply ineffective. While some tools such as the affordable software programme *Lexibot* are available to assist in collection from the "deep web", considerable time is spent in the identification and analysis of open sources relevant to the information requirement. For this reason, a major aspect of the OSINT support process is the skilled creation of Internet Link Tables that serve as a ready reference for the commander or staff officer who desires to rapidly scan external information sources without necessarily requesting a report. This browsing endeavor can often help the commander or staff principal reflect on their requirements and better articulate their next demands for finished OSINT. An Internet Link Table should generally be in the form of a Table, such as is illustrated In Table 5 above. By using the Word Table feature, this allows the sorting of the information based on either the Rank or Weight assigned to the site, the URL or title of the site, or the description category of the site. Over time, as various NATO components cooperate and share Link Tables with other allies forces such as the various regional Joint Intelligence Centers, a very comprehensive directory of web resources, one that is tailored to NATO's needs, should emerge.

Ranking	Link	Source
10	http://allafrica.com/libya/	**All Africa News – Libya –** Up-to-date news on Libya, in English and in French.
10	http://memory.loc.gov/frd/cs/lytoc.html	**Library of Congress Libya Country Study** – Excellent, in-depth country study
10	http://members.aol.com/LibyaPage/	**Libya Resources on the Internet –** Excellent, comprehensive site, includes news, Qadhafi info, maps and satellite photos, military and intel, etc.
10	http://www.un.int/libya/	**The Permanent Mission of Libya to the UN** Website **–** Includes press releases & statements, ambassador's remarks and links.
10	http://www.nfsl-libya.com/	**The National Front for the Salvation of Libya** - The NFSL is an opposition movement against the dictatorial regime of Qadhafi in Libya, and was formed in October 1981.
8	http://www.libyamazigh.org/	**Libyan Amazigh** site. Contains info on Libya's Amazigh (Berber) culture, language and history.
8	http://www.libyaonline.com/index.html	**Libya Online** Website – Contains basic facts about Libya, tourism, business, arts, literature and sports.

Table 5 - Example of Internet Link Table

Distance Learning

The Internet, while rendering a major service to those who would like to share information efficiently and also interact inexpensively with diverse people all over the world, has also reduced the productivity of even experienced personnel. Constant interruptions and distractions through diversions to less important information are

core factors. For this reason, there is an urgent need for Distance Learning modules on all countries and topics that are of interest to NATO. The objective is to ensure that all new personnel, and especially new action officers, have an online resource that can serve as a sophisticated turnover file and reference point. This is also a place where unclassified biographic information can be made available, and where annual reviews of each country or topic can be placed.

The U.S. Pacific command initiative known as the Virtual Information Center is an good example of this process. It can be accessed at www.vic-info.org.

Figure 14 - Homepage of US PACOM OSINT Centre

Expert Forums

A number of software programs exist with which to manage a variety of Expert Forums, including private teams with their own newsletters, calendars, and automated email alerts whenever new information is posted. One of the most popular is the Alta Vista Forum. One of the newest, with powerful security features, is offered by Groove Inc. (www.groove.net) and represents the emerging shift in communications and computing power away from centralized server farms toward what is known as "peer to peer" edge units.

Expert Forums can be internal, external, or some combination of the two. Once experts have been identified, they may be invited to join the Expert Forum sponsored by any NATO element. This should be done with the understanding that they will contribute their time and insights on an occasional basis, in return for being granted access to the OSINT being produced by the NATO element sponsoring the Expert Forum. Such a forum can also be a place where individual experts "audition" for short-term consulting contracts and where the biographies of available efforts can be made available for anonymous review by potential NATO employers.

Expert Forums should consist of several parts, all of them of potentially great value to the NATO OSINT process. First, while it is possible to register anonymously for a forum, the greatest value comes from an open registration that includes a photo, biographic note, and complete contact information. Second, the forum will quickly self-organize, with a variety of topics to which an individual can not only contribute observations, but to which they can upload documents, images, even video. The flexibility and scalability of these forums cannot be overstated—but they do have one major flaw: at this time, it is not possible to apply visualization or other technologies to the varied contents of a forum—each item must be copied down to a master database first.

Soon the technology will be available to index and abstract all information contributed to a forum, at which time the best of all worlds will be available: distributed experts able to cast a wide net, and a centralized "banking" function for information freely contributed by various parties. Third, the forum permits the rapid organization of private working groups, and offers calendar, newsletter, and other

coordination features. Fourth and last, the forums can provide an automatic email alert to any member whenever new information is posted to a topic of interest to them, relieving them of the need to constantly check the forum site.

SECTION F. DISSEMINATION AND EVALUATION

Overview

The major difference between OSINT and the other intelligence disciplines is that the latter are inherently classified: OSINT can be shared with *anybody* that the commander deems appropriate, without having to request security or political clearances.

This makes it extraordinarily valuable in non-article V operations as well as in dealing with civil sector coalition partners—including NGO that traditionally distrust the military in general and intelligence professionals in particular. OSINT has become even more valuable in the 21st Century, as there has been a major change in the over-all C^4I paradigm.

As NATO continues to evolve and transform itself in response to the many new challenges, the importance of OSINT will continue to evolve. These new challenges include non-traditional non-military challenges requiring coordinated action with non-governmental and humanitarian relief organizations.

OSINT appears to offer a very substantial advantage as a prime intelligence source and method with which to achieve consensus and a common understanding of the shared area of operations.

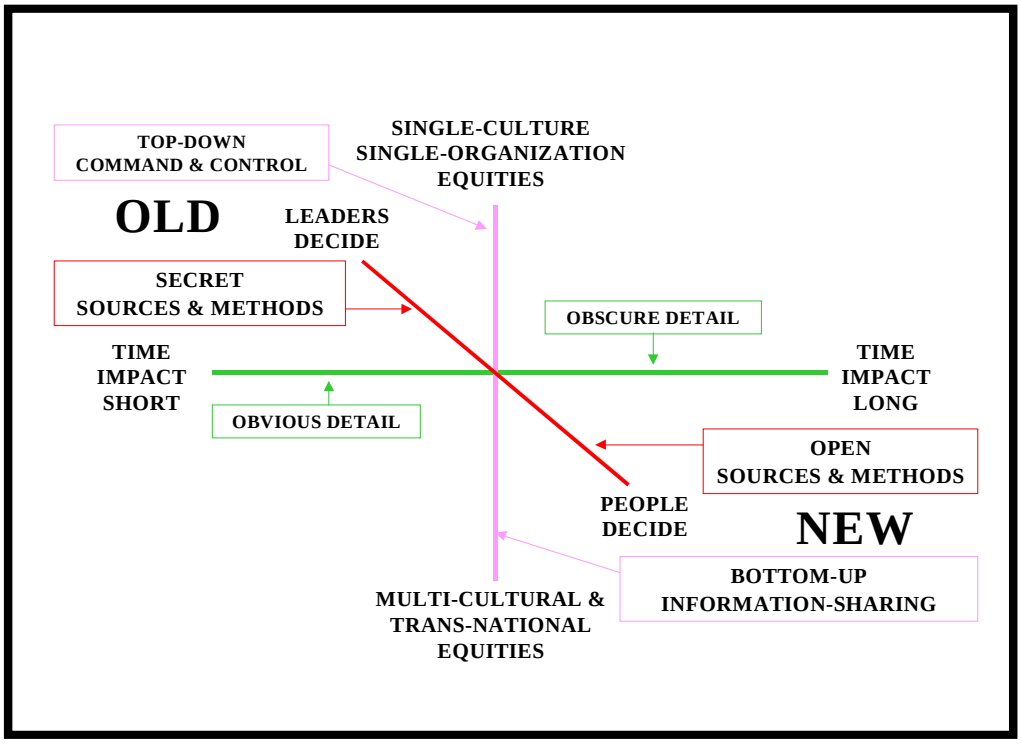


Figure 15 - Emerging Paradigm for Information Sharing

Dissemination Methods

Once open source information has been developed into OSINT, it can be disseminated via the NATO WAN in a "push" mode, or it can be "pulled" off on demand.

The limitations placed on its dissemination are based on the security policies of the organization producing it. While some OSINT products may be shared openly, others may provide details of interests or intentions and should therefore be restricted in their dissemination. The dissemination policy should be driven by the mission requirements. The approach should nonetheless be flexible to fully leverage the ability that the production of OSINT products provides for the engagement of non-NATO elements in security discussions or the development and dissemination of a common view of the operating area.

Within the NATO Intelligence Architecture, options exist for the dissemination of OSINT products via the classified NATO WAN or directly through the Internet. The advantages of the NATO WAN are the direct access afforded to the operations and policy staffs at all levels, including deployed units, as well as the security afforded by the use of a classified system. The principal disadvantage of the NATO WAN for OSINT dissemination is the necessary separation of the products from their source material. Without a direct linkage between an OSINT product and the sources of information, the recipient is less able to drill deeper for additional information, reach the original author, or further evaluate the original sources of the information.

Another option is the use of a Virtual Private Network (VPN). A VPN is a restricted community of interest that communicates on the Internet but use security safeguards to limit the access from others who are not members. By using a VPN, OSINT products can be accessed safely and with working links directly to the original source material. Link tables can also be maintained that enables the rapid collection of information. Other OSINT centres within NATO member countries have direct access to the Internet; few have access to the NATO WAN. A VPN provides the means with which to exchange OSINT products with other OSINT centres across NATO. Finally, the use of a VPN provides the means with which to disseminate OSINT products with non-NATO elements such as NGOs and other international organizations as mission requirements demand.

For these reasons, exploring the feasibility and desirability of a VPN to support the NATO OSINT Initiative remains a priority. SACLANT has begun a trial VPN with the U.S. Open Source Information System (OSIS) to examine the viability of linking NATO OSINT production centres with U.S. OSINT holdings.

Virtual Intelligence Community

The NATO OSINT initiative is the first major multi-national OSINT initiative ever undertaken. While there is much still to learn from those member nations that adopted OSINT as an independent discipline in the 1990's, as well as from the emerging business intelligence community (such as represented by the Society of Competitive Intelligence Professionals at www.scip.org), it is NATO that is leading in the establishment of formal doctrine and tables of organization and equipment specifically earmarked for OSINT. It is helpful, in contemplating this activity, to understand that there is a substantial but still fragmented community of interests with whom NATO could co-develop many OSINT initiatives. This community is illustrated in Figure 16.

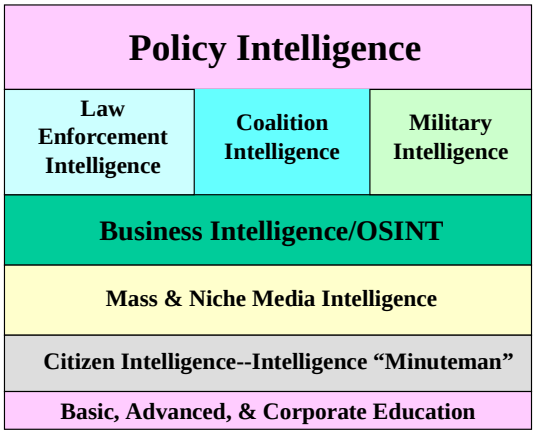


Figure 16 - Elements of a virtual intelligence community

As commanders and their staff evaluate their needs for OSINT, and new methods as well as budget deficiencies, SCs and subordinate commands should seek to establish a constant process of interactive liaison with each of the elements of the "virtual intelligence community" shown here. In this fashion, NATO intelligence could benefit from a greater OSINT effort that cuts across bureaucratic and cultural boundaries, and leads to improved cost efficiencies and new forms of information sharing.

CHAPTER IV
OSINT AND THE EMERGING FUTURE INTELLIGENCE ARCHITECTURE OF NATO

SECTION A. BLENDING OSINT INTO THE ALL-SOURCE PROCESS

Overview

Apart from the importance of OSINT as a means of establishing consensus and a common view with external parties about the shared area of operations, OSINT is absolutely vital to the all-source intelligence process. OSINT provides the historical background information, the current political, economic, social, demographic, technical, natural, and geographic context for operations, critical personality information, and access to a wide variety of tactically useful information about infrastructure, terrain, and indigenous matters. The relationship between OSINT, the traditional collection disciplines, and all-source analysis is shown in Figure 17.

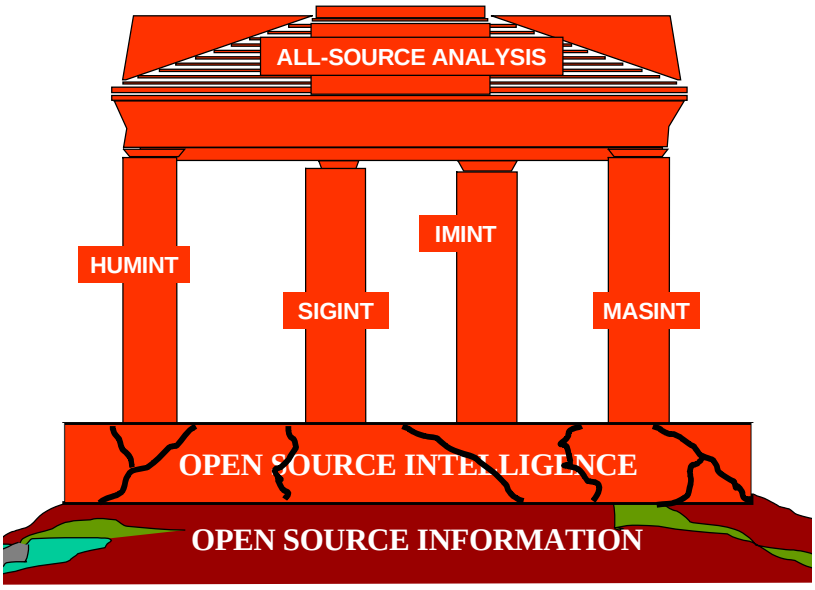


Figure 17 - Open Source - All-Source relationship

Cracks are shown in the OSINT foundation to emphasize that this vital element of the all-source intelligence process has been too long neglected. Following the publication of the Alliance's Strategic Concept in April 1999, OSINT is even more important. NATO, along with other international organizations, is now striving to understand ethnic conflict, water and food scarcity, mass migrations, the collapse of public health across entire continents, transnational crime, and all of the small wars—and the potential threat of large wars—that remain a traditional responsibility. OSINT can and should be integrated into every aspect of the all-source process, from collection through production.

Nations and NATO commands differ fundamentally in their approaches towards OSINT. Both begin with intelligence needs that lead to the generation of intelligence requirements. The approaches diverge at that point. While nations may use OSINT to guide classified collection, NATO rarely has classified collection means beyond the tactical level and those assets are largely restricted to theatres in which forces are already deployed.

NATO commands can use OSINT-V to satisfy intelligence gaps for a large number of its intelligence needs. While nations are able to turn to classified intelligence collection, NATO can and should use the OSINT process described as the first step in its collection process. Too often, NATO commands have defaulted to sending RFIs to nations rather than seeking first to address their intelligence requirements themselves. The range of open sources now within reach of NATO intelligence staffs provides other options.

The new Strategic Concept articulated a vision for the Alliance that is largely focused on non-traditional operating areas and transnational threats. The intelligence services of the NATO member countries are also struggling to deal with a similar problem set. These areas and interests, while not well covered by traditional intelligence production are well addressed in open sources. Rather than relying solely upon nations for intelligence products, NATO intelligence staffs should develop their own network of open sources as the starting point for the compilation of their intelligence assessments.

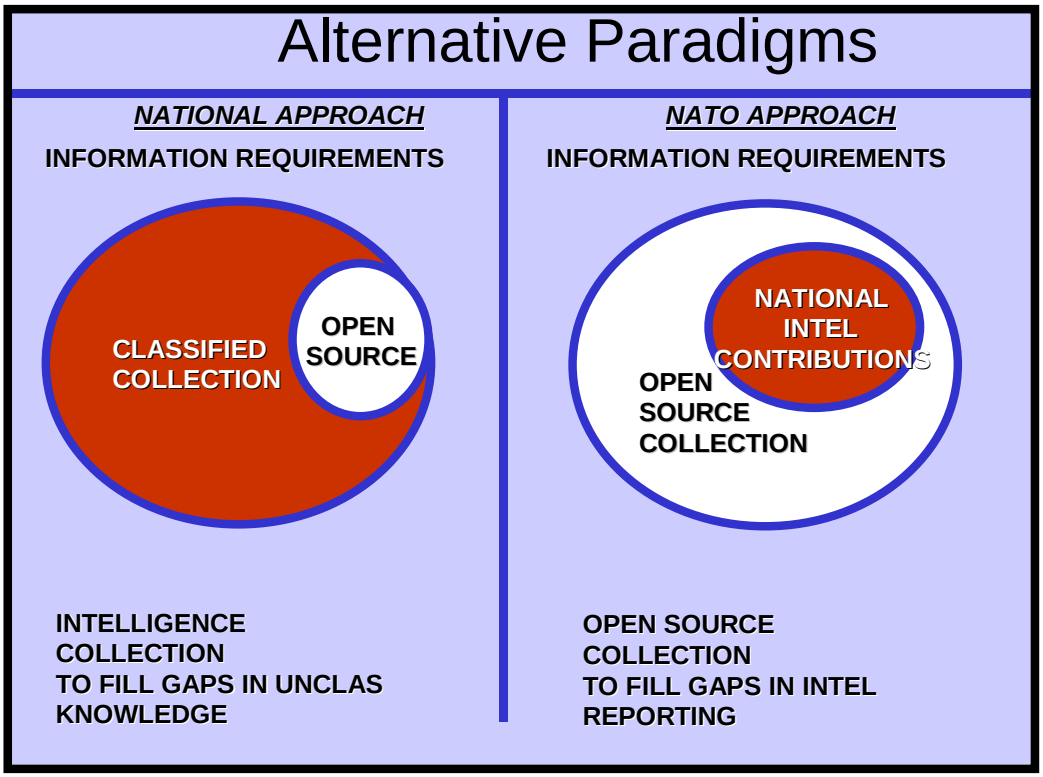


Figure 18 - Alternative Paradigms between NATO and National OSINT Approaches

Direction

Open information sources are as easy for NATO leadership to access as they are for their intelligence staffs. No longer are intelligence staffs in a position to regulate the flow of relevant information to the commander or his staff. Virtually all decision-makers make regular use of open sources to varying degrees. Knowledge of those sources routinely consulted by the staff principals is an important means with which to stay ahead of their intelligence needs.

Rather than attempting to stem the use of open sources by the commander or his staff, an effective OSINT effort facilitates it. Intelligence staffs at both Strategic Commands (SCs) have access to specialized information retrieval tools and commercial sources. In addition, both SCs are in a position to provide training and advice on the effective retrieval of information from open sources. An OSINT process should include the provision of validated information sources for each issue that affects the command. The provision of Link Tables as well as quality assessments of other information sources is an essential OSINT product.

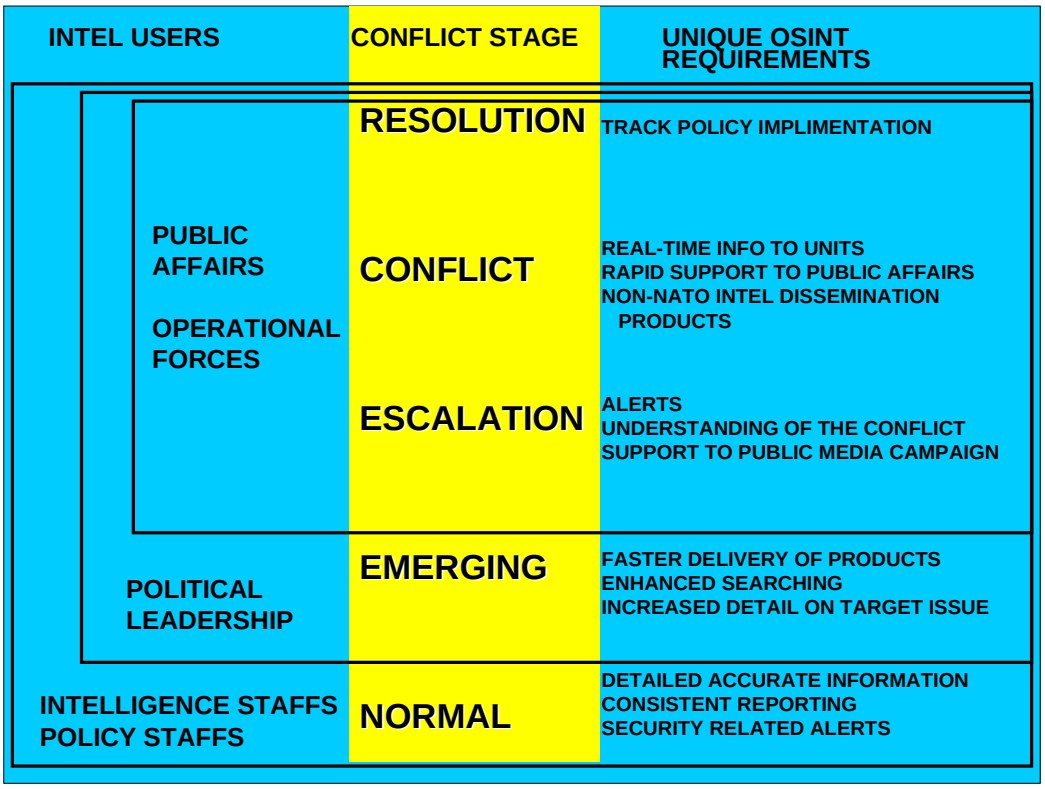


Figure 19 – Unique OSINT Requirements across the Conflict Spectrum

Typically, informed decision-makers make reasoned requests for intelligence. While not always the case, this statement generally holds true. With an appreciation for what is widely known, intelligence users will tend to restrict their requests to that information which they do not already have available to them.

OSINT can support the direction phase of an

all-source intelligence effort through discovery of an issue or providing context with which to understand issues.

The intelligence problem varies depending on the nature of the issue being addressed, which elements of the staff are engaged and what degree of information is required. Figure 19 shows a representative range of information products that a robust OSINT capability can provide.

Assuming an OSINT capability is in place in advance of a crisis, it is likely that the leadership will have had access to quality open source products prior to the onset of mission requirements. In that case informed RFIs can be expected. If there is no familiarity with the issue, decision-makers can be directed to either established OSINT products or open sources of information that can be made available through access to an information portal such as a VPN of another network. Finally, an OSINT collection effort can be initiated to quickly produce relevant background information. This immediate OSINT effort will quickly establish what is easily known about the subject and guide the priorities for classified collection and all-source production.

Collection

Within the intelligence cycle, the collection phase includes the translation of the intelligence need into a collection requirement, the definition of a collection strategy, the selection of the collection sources and the actual information collection. Open sources should be the first recourse in the collection process. OSINT saves money in reducing unnecessary classified collection. In a NATO context, it saves time as RFIs to nations require sufficient lead-time for them to be properly addressed.

While open source information is not free, the costs pale in comparison to those of the classified collection disciplines. If open sources can be collected to produce an OSINT product that addresses completely or to a large degree the intelligence need, classified collection resources can be more effectively deployed elsewhere.

While nations have classified collection capabilities, these are expensive and must always be used wisely. NATO has no tasking authority over national intelligence collection capabilities. Its reliance upon intelligence contributions from nations makes it incumbent upon its intelligence staffs to know what can be known without technical collection.

Open sources have always been used by intelligence organizations. Open sources have typically been referred to as *collateral reporting*. In fact, all single source intelligence disciplines refer to information provided by another intelligence discipline as *collateral reporting*.

However, when this collateral reporting is maintained with a systematic disciplined approach as discussed in this OSINT Manual, the “collateral” grows in its own utility. Instead of being acquired once and used by one intelligence element, it is acquired once and applied across a broader range of the intelligence process from streamlining collection to increasing dissemination.

OSINT’s four main contributions to classified collection are: tip-off for classified sources; targeting of those sources; context and validation to better understand material collected from classified sources, and; providing plausible cover to protect the classified source.

Tip-off.

- Open sources are particularly well suited to providing *tippers* for other collection disciplines. The reduction in the number of denied areas since the end of the Cold War and the advent of cheap international transportation options have enabled greater media access than ever before. Internet NEWSGROUPS, wire services and other traditional print and broadcast media are all within the reach of anyone.

- The Internet remains a primary means with which to gain access to these sources. While traditional print and broadcast media are restricted in the amount of information that they can provide, the Internet has provided virtually limitless dissemination capabilities for information producers. Rather than the editor's selection of stories, the Internet provides the means with which to gain access to all stories filed with all of the wire services depending on the degree of access that is purchased.

- A number of services provide news alerts that are either free of charge or low cost. Non-traditional sources of information include those who witness important events and who post messages on the Internet about what they have seen. While prone to disinformation, this is another source of information that must be evaluated like all others. Those who witness an event and publish on-line or forward emails to their communities of interest can provide the first indication of an event even before media publication.

Targeting.

- While OSINT will often be able to address elements of an intelligence problem quickly and efficiently, OSINT will never invalidate the need for classified collection capabilities.

- When intelligence gaps can be addressed without the need to task classified collection sources overall demand upon limited collection resources decreases. This permits concentration of effort on those issues that can only be discovered through classified collection.

- This model of complementary collection permits both open and classified sources to be optimized for a particular intelligence problem, while at the same time, affording the all-source analyst the ability to use the classified collection products to validate the OSINT products.

Context/Validation.

- Supplemental open source reporting can provide the means with which to place classified reporting into context. Classified reporting, particularly current intelligence reporting, often fails to provide the necessary background information with which to tailor the information to the needs of the recipient or to explain the nuances of the situation.

- While imagery can provide knowledge of ships alongside piers, additional information from open sources can provide an understanding of the cargo that the port handles or the schedule of the ship. Similarly, UN reporting on agriculture production shortfalls in a particular country will give insight into population movements detected with national technical means.

Plausible Cover.

- OSINT is particularly useful in protecting classified sources and methods. The discovery of an open source that corroborates classified

Figure 20 - Commercial imagery of San Diego naval base

reporting may increase the releasability of the initial information by providing a plausible alternate source. This also has applicability to the staffing of requests for the sanitation of classified reporting.

- A thorough understanding of information that is available in unclassified channels facilitates the discovery of plausible alternate sources to classified intelligence reporting. This ultimately increases the ability of intelligence staffs to release intelligence information to non-NATO elements within missions.

Processing

The objective of intelligence processing is the creation of an intelligence product that is value-added, actionable information tailored to a specific user. All-source analysis with its fusion of all relevant and validated sources of information remains the best means to convey intelligence to the user. This process includes both classified and OSINT reporting as appropriate. In most cases, NATO will serve as one element of an international crisis response. Experience has shown that these operations likely include the leading of a broader coalition alongside non-NATO troop contributing nations (NNTCNS). The processing of intelligence products to support the information needs of both the NATO-led force and the international response elements is greatly enhanced with a robust OSINT capability.

Intelligence products can be prepared with a tear-line – classified intelligence restricted in its dissemination above the line and sanitized information that can be more broadly disseminated below the line.

OSINT–V products can be produced specifically tailored for the broader coalition audience but validated by the all-source process. During actual operations, the need to disseminate to non-NATO elements includes not only their operational forces, but also their political liaison elements at NATO headquarters in Brussels.

Figure 21 - Nature of international operations

The maintenance of information sources that can be disseminated outside of NATO channels can often prove essential to both establishing a common view of the operating area and initiating an exchange with other entities that can contribute to the understanding of an issue.

Dissemination

As stated earlier, OSINT is itself optimized for dissemination through VPNs. This enables ready access to the original source material, direct interaction with other related open sources and access to other OSINT producers.

The dissemination of OSINT products as stand-alone intelligence products on classified systems should also be encouraged. OSINT as either stand alone products or as collateral reporting adds to the body of knowledge on a particular issue. Intelligence staffs at all levels should be able to benefit from the effort put into their production. It is rare that all subordinate commands will have access to every intelligence system. Thus, efforts should be made to ensure that products are available on all intelligence dissemination systems as security constraints permit.

Typically, the lower the classification of an intelligence product the wider is its uses. If decision-makers are able to leave their offices with an intelligence product, it is more likely that it will receive undisturbed attention. OSINT products provide the means to place high quality low-classification or unclassified products in the hands of intelligence users. This is only possible if they are disseminated on systems typically used to deliver other forms of intelligence.

The objectives of a robust OSINT capability should be to increase the range of information available to intelligence users and to facilitate interaction with non-NATO elements as appropriate. The dissemination options developed should seek to achieve these two objectives.

APPENDIX A: GENERAL REFERENCE LINK TABLE

Maps:

World Ports	http://www.world-ports.com/
United Nations	http://www.un.org/peace/kosovo/pages/kosovo1.shtml
CIA World Factbook	http://www.odci.gov/cia/publications/factbook/indexgeo.html
Quick Maps	http://www.theodora.com/maps/abc_world_maps.html
CNN Video Select	http://europe.cnn.com/video/netshow/
The Place For Maps	http://www.maps.com/?AID=41160&PID=186662
Map Quest	http://www.mapquest.com/
Expidia.com	http://www.expedia.com/pub/Agent
Media Maps.com	http://media.maps.com

News:

NBC Daily	http://www.nbc.com/
Bloomberg	http://www.bloomberg.com
MSNBC	http://www.msnbc.com
CNN Videoselect	http://europe.cnn.com
Fox News	http://www.foxnews.com
BBC Monitoring	http://news.monitor.bbc.co.uk/
BBC NEWS	http://news.bbc.co.uk/
CBS NEWS	http://www.cbs.com/daytime/bb/show_update/update.shtml
CNBC Dow Jones Business Video	http://cnbcdowjones.com/msnbc
CNET Today	http://news.cnet.com
ABC News	http://abc.go.com
CNN	http://www.cnn.com
The Sunday Times	http://www.information-britain,co.uk/news.sundaytimes.htm"
News Now 1401	http://www.newsnow.co.uk/
MSN News	http://www.msn.com
Real Radio	http://realguide.real.com/tuner/?
ABCNews	http://abcnews.go.com/
Business Journal	http://business.netscape.com/business/main.tmpl
Fox News	http://www.foxnews.com/
International News	http://www.internationalnews.com/
AJR News Link	http://ajr.newslink.org/
ITN News British	http://www.itn.co.uk/
The World News	http://www.theworld.org/
Out There News	http://www.megastories.com/index.shtml
CNN International	http://europe.cnn.com/CNNI/
The Times	http://www.thetimes.co.uk/
LA Times	http://www.latimes.com/
Jerusalem Post	http://www.jpost.com/
Belfast News	http://www.belfasttelegraph.co.uk/index.shtml
The Washington Post	http://www.washingtonpost.com/
South China Morning Post	http://www.scmp.com/
The Japan Times	http://www.japantimes.co.jp/
Yahoo	http://www.yahoo.com
The CNET Channel	http://channel.cnet.com/Channel/Intro/index.htm
The Wall Street	http://interactive.wsj.com/ie4intro/index.htm

Conflict:

United Nations High Commission For Refugees	http://www.unhcr.org
Weapons Of Mass Destruction	http://www.fas.org/irp/threat/wmd_state.htm
Terrorism Research	http://www.terrorism.com/index.shtml

Counter Terrorism	**http://www.state.gov/www/global/terrorism/**
Intelligence Net	**http://www.intellnet.com**
Federation of American Scientist	**http://www.fas.org**
War Information	**http://www.psycom.net/iwar.1.html**
China's Military Developments	**http://www.commw.org**
Kosovo Info	**http://perso.respublica.fr/infokosovo/**
Institute for Global Communications	**http://www.igc.org**
Anti War Home Page	**http://www.nonviolence.org/archivedsites/iraq/**
Missle, Threats & Response	**http://www.cdiss.org/tempor1.htm**
Modern Day Piracy	**http://www.geocities.com/Tokyo/Garden/5213/modern.htm**
KORB Marine Links	**http://www.pg.gda.pl/~korab/kor_lnk.html**
Piracy Centre	**http://www.iccwbo.org/ccs/menu_imb_piracy.asp**
The Panama Canal	**http://www.pancanal.com/eng/index.html**
Royal Australian Navy Sites	**http://www.navy.gov.au/html/links.htm**
Royal Navy Association	**http://www.royal-naval-association.co.uk/page6.htm**

Regional Information:

CIA World Factbook	**http://www.odci.gov/cia/publications/factbook/indexgeo.html**
Geo Spatial Information	**http://www.geoplace.com/**
Geographic Learning Site	**http://geography.state.gov/htmls/plugin.html**
Association For Geographical Information	**http://www.agi.org.uk/**
Salam Iran	**http://www.salamiran.org/IranInfo/General/Geography/**
Limes Geo review	**http://www.limesonline.com/doc.navigation**

Reference:

Britannica	**http://britannica.com/**
Dictionary	**http://Dictionary.com**
Every Rule	**http://Everyrule.com**
FBIS	**http://199.221.15.211/**
Central Intelligence Agency	**http://www.cia.gov/**
Indian Naval Review	**http://www.janes.com/defence/naval_forces/gallery**
Bureau for International Narcotics and Law Enforcement Affairs	**http://www.state.gov/www/global/narcotics_law/**
Archive Site for State Department information	**http://www.state.gov/index.html**
Naval Technology	**http://www.naval-technology.com/index.html**
Janes Naval Forces	**http://www.janes.com/defence/naval_forces/index.shtml**
Encyclopedia	**http://Libraryspot.com**
World Fact Book	**http://Worldfactbook.com**
The Intelligence Community	**http://www.odci.gov/ic/**
One World	**http://www.oneworld.net/**
Yahoo	**http://www.yahoo.com**
Lloyds List	**http://www.lloydslist.com**
Ask Oxford	**http://www.askoxford.com/**
(WMD) Weapons Of Mass Destruction	**http://www.fas.org/irp/threat/wmd_state.htm**
Incident Response	**http://www.llnl.gov/nai/rdiv/rdiv.html**
Conference For Middle East Peace	**http://www.cmep.com/**

APPENDIX B: TRAINING LINK TABLE

Below are a few of the essential references that are available online. Please note that the NATO guide *Intelligence Exploitation of the Internet* is also available online at the SACLANT Intelligence homepage on the NATO WAN. This publication is regularly updated with the best resources available to guide in the use search strategies and tools to exploit open sources available on the Internet. The Open Source Intelligence Proceedings include over 5,000 pages from over 500 international authorities including the (then) Director General of the International Red Cross and many other European and Asian experts, and comprise the "information commons" on the state of the art for open source intelligence.

OSINT Presentation to SHAPE/PfP Flags	http://www.oss.net/Papers/white/SHAPE.ppt
Information & Intelligence Bibliography	http://www.oss.net/Papers/white/23-BibliographyAnnotated.rtf
Eight Self-Paced OSINT Lesson Plans	http://www.oss.net/DispFrame.html?Papers/training/index.html
Creating an OSINT Cell (DIA Report)	http://www.oss.net/DispFrame.html?Papers/white/DIAReport.html
Business Intelligence Primer (1994)	http://www.oss.net/DispFrame.html?Papers/white/THETHEORYANDPRACTICEOFCOMPETITORINTELLIGENCE.html
Open Source Intelligence Proceedings	http://www.oss.net/Proceed.html
Index to OSINT Proceedings	http://www.oss.net/Papers/white/index.rtf
OSINT and the Military	http://www.oss.net/Proceedings/95Vol1/aab0aw.html
Canadian Intelligence Studies	http://www.sfu.ca/igs/CASIS/
Come Back Alive "Ground Truth"	www.comebackalive.com/df/index.htm
Future of Intelligence	www.future-intel.it
History of Intelligence	http://intelligence-history.wiso.uni-erlangen.de
Intelligence Resource Program	http://www.fas.org/irp/index.html
Links to International Media	http://www.esperanto.se/kiosk/index.html
Literature of Intelligence	http://intellit.muskingum.edu
Open Directory Project	http://dmoz.org/
Strategic Intelligence	http://www.loyola.edu/dept/politics/intel.html
Form for Evaluating the Value of Web Pages	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/EvalForm.pdf
Internet Training Course by Russ Haynal	http://navigators.com/fbis.html
Berkeley University Tutorial for Finding Information on the Internet	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/FindInfo.html
Search Techniques for the Invisible Web	http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html#Table
Techniques for “Searching Upstream”	http://websearch.about.com/library/weekly/aa061101a.htm?once=true&

APPENDIX C: CATEGORIES OF MISPERCEPTION AND BIAS

Evoked-Set Reasoning: That information and concern, which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.

Prematurely Formed Views: These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.

Presumption that Support for One Hypothesis Disconfirms Others: Evidence that is consistent with one's preexisting beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.

Inappropriate Analogies: Perception that an event is analogous to past events based on inadequate consideration of concepts or facts or irrelevant criteria. Bias of "Representativeness".

Superficial Lessons From History: Uncritical analysis of concepts or event, superficial causality, over-generalization of obvious factors, inappropriate extrapolation from past success or failure.

Presumption of Unitary Action by Organizations: Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismisses accident and chaos. Ignores misperceptions of others. Fundamental attribution error possibly caused by cultural bias.

Organizational parochialism: Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Can result from functional specialization. Groupthink or stereotypical thinking.

Excessive Secrecy (Compartmentation): Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or caused organizational parochialism.

Lack of Empathy: Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.

Mirror-Imaging: Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.

Ignorance: Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, and denial of reality, rational-actor hypothesis (see next entry).

Rational-Actor Hypothesis: Assumption that others will act in a "rational" manner based on one's own rational reference. Results from ethnocentrism, mirror imaging, or ignorance.

Denial of Rationality: Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behavior or decision making. Opposite of rational-actor hypothesis. Can result from ignorance, mirror imaging, parochialism, or ethnocentrism.

Proportionality Bias: Expectation that the adversary will expend efforts proportionate to the ends he seeks. Interference about the intentions of others from costs and consequences of actions they initiate.

Willful Disregard of New Evidence: Rejection of information that conflicts with already-held beliefs. Results from prior commitments, and/or excessive pursuit of consistency.

Image and Self-Image: Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by self-absorption and ethnocentrism.

Defensive Avoidance: Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.

Overconfidence in Subjective Estimates: Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.

Wishful Thinking (Pollyanna Complex): Hyper-credulity. Excessive optimism born of smugness and overconfidence.

Best-Case Analysis: Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.

Conservatism in Probability Estimation: In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to reexamine established tenets. Tendency to seek confirmation of prior held beliefs.

Worst-Case Analysis (Cassandra Complex): Excessive skepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interest or policy preferences.

Source: Lisa Krizan. *Intelligence Essential for Everyone*. Washington D.C. Joint Military Intelligence College, June 1999.

APPENDIX D. LIST OF ABBREVIATIONS

AIIB – Association of Independent Information Brokers
AOO - Area of Operations
API - Application Program Interfaces
BBC - British Broadcasting Corporation
COSPO - Community Open Source Program Office
EEI - Essential Elements of Information
FBIS - Foreign Broadcast Information Service
ICRC - The International Committee of the Red Cross
ISPs - Internet Service Providers
MCCIS – Maritime Command and Control Information System
NATO - North Atlantic Treaty Organization
NDA - Non-Disclosure Agreements
NGO - Non-Governmental Organization
NNTCNS - Non-NATO troop contributing nations
OPSEC - Operational Security
OSIF - Open Source Information
OSINT - Open Source Intelligence
OSO - Open Source Officers
PfP - Partnership for Peace
RFI - Requests for Information
SACEUR - Supreme Allied Commander, Europe
SACLANT - Supreme Allied Commander, Atlantic
SAR - Synthetic Aperture Radar
SC - Strategic Commands
SCI - Science Citation Index
SME - Subject-Matter Experts
SSCI - Social Science Citation Index
STN - Scientific and Technical Network
UN - United Nations
VPN- Virtual Private Network
WEU - Western European Union

FEEDBACK

This manual is intended to be a living document. It represents the first attempt by NATO to place OSINT within the broader context of intelligence efforts. The intention is to subject this publication to regular review and updating to reflect new sources and methods for open source exploitation.

As such, feedback is welcome in any form. Comments, amendments, additions or errors can be reported either with the form below or via email to rsc@saclant.nato.int.

Name: _____

Parent Command: _____

Telephone number: _____

Email address: _____

Comment:

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

Fax to: HC-310
SACLANT Intelligence Branch
Norfolk, VA
757-445-3572