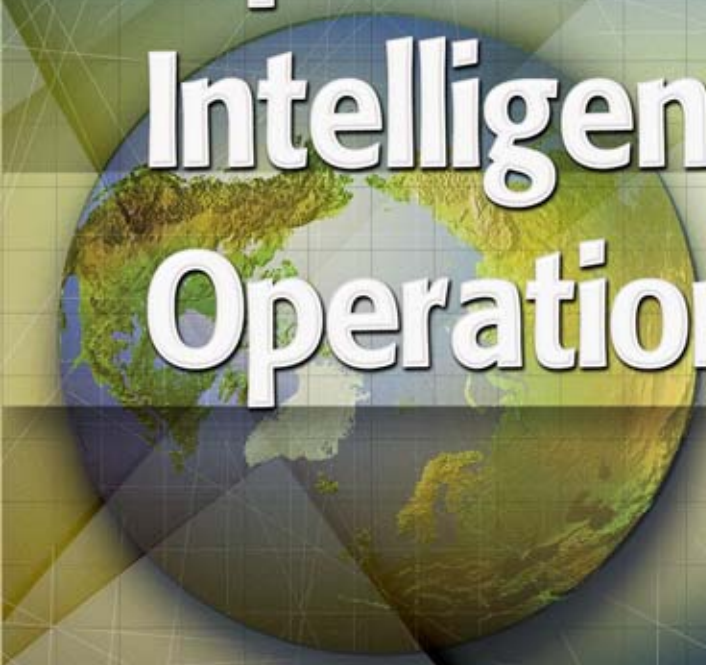
FOR OFFICIAL USE ONLY

US ARMY INTELLIGENCE AND SECURITY COMMAND
OFFICE OF THE ASSISTANT CHIEF OF STAFF, G-3

INSCOM Open Source Intelligence (OSINT) Operations Handbook

May 2003



Note: This OSINT Handbook is intended to be a living document and will be updated as operational necessity requires.

FOR OFFICIAL USE ONLY

UN030577

DEPARTMENT OF THE ARMY
UNITED STATES ARMY INTELLIGENCE AND SECURITY COMMAND
8825 BEULAH STREET
FORT BELVOIR, VIRGINIA 22060-5246

IAOP

13 May 2003

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: INSCOM Open Source Intelligence (OSINT) Operations Handbook

1. One of INSCOM's goals is to aggressively exploit the Global Information Environment (GIE) to provide all relevant, accurate, and timely open source information to Army decision makers, commanders at all levels, and force developers as standalone documents or fused into all-source products anywhere, anytime.

2. The purpose of this memorandum is to distribute the enclosed INSCOM OSINT Handbook aimed at improving INSCOM MSC's collection, processing, analysis and dissemination of Open Source Intelligence that impacts the Command's wide-range of operational activities.

3. While this OSINT Handbook cannot be all inclusive, it does provide a good reference and a starting point for focusing on this critical discipline. It is hoped that MSC inputs to this Handbook will improve its future utility and coverage.

4. INSCOM's POCs for working updates to this Handbook is LTC Steve Martin (703-706-1830; steve.martin@inscom.army.mil) and Mr. Ed Dandar, SYTEX (703-706-2506; efdanda@inscom.army.mil).

Encl
as

NEAL F. SIEBERT
ACofS, G3

DISTRIBUTION:
A, B, C

US Army Intelligence and Security Command
Office of the Assistant Chief of Staff, G3

INSCOM
Open Source Intelligence (OSINT)
Operations Handbook

May 2003

Note: This OSINT Handbook is intended to be a living document and will be updated as operational necessity requires.

TABLE OF CONTENTS Page

TABLE OF CONTENTS (Cont)

PREFACE

Army policy is to provide relevant, accurate, and timely Open Source Intelligence (OSINT) to commanders at all levels by integrating OSINT into all disciplines and functions; exploiting the information age; and making OSINT a vital intelligence resource. The intent is to develop and implement an OSINT process; actively recruit and retain skilled intelligence professionals capable of leveraging OSINT; and to instill Army confidence in OSINT by demonstrating its value added.

The acronym OSINT is used in this manual to represent open source intelligence and it is important to distinguish OSINT from the other "INTS" (HUMINT, SIGINT, IMINT and MASINT) that are collection activities that produce classified products.

OSINT is intelligence developed from open, unclassified literature. Researchers in industry and the academic world; journalists; public and private media enterprises; local, state, federal and foreign governments; and non-governmental organizations produce a continuous flood of information. The accelerating expansion of the Internet and global information explosion requires intelligence professionals to better leverage OSINT in meeting customer requirements.

The Intelligence Community defines OSINT as publicly available information that any member of the public could lawfully obtain by request or observation, as well as, other unclassified information that has limited public distribution or access. It also includes any information that may be used in an unclassified context without compromising national security or intelligence sources and methods. Information that is not publicly available may implicate other legal requirements relating to its collection, retention, and dissemination.

This handbook provides an overview of the global open source environment, provides guidelines for OSINT acquisition, and prescribes procedures for OSINT exploitation by INSCOM intelligence professionals. The objective of this publication is to provide a framework for understanding the OSINT discipline and process, improving its use, and timely satisfaction of customer information needs.

ACKNOWLEDGEMENTS

The US Army Intelligence and Security Command (INSCOM) would like to acknowledge a number of organizations whose OSINT contributions have been invaluable in preparing this handbook. In particular, INSCOM wants to recognize the November 2001 NATO Open Source Intelligence Handbook and the contributions made to it by Open Source Solutions, Inc in its preparation. We would also like to acknowledge the assistance provided by Focused Research International, Inc., the Army's Foreign Military Studies Office, INSCOM Interns, the former CW4 Alan Devoe Tompkins, and members of SYTEX, Inc. in the final preparation of this handbook.

1. 0 INTRODUCTION

1. 1 **Perpetual Challenge**.

a. The continuing 21st Century information explosion and the increasingly ready access to information via public domain media has caused a review and evaluation of the potential of Open Source Information (OSI) for intelligence purposes. A key goal for Army Transformation is ensuring Army closes the gap in 21st Century information dominance.

b. This includes developing a robust Open Source Intelligence (OSINT) capability in means, organization, and trained personnel to exploit the Global Information Environment. As the Army moves toward 2010, it will be strongly driven by technology and the Information Age.

c. The ongoing Military Technology Revolution (MTR) will provide a framework for explaining and guiding the changes that are occurring. The successful application of military power will be directly proportional to the effectiveness of intelligence and the execution of information operations. Information Technology (IT) has increased in complexity and capability and has become indispensable to combat operations. IT has become a weapon in its own right and is viewed as a "handmaiden to the instruments of war."

1.2 **The Global Information Environment (GIE)**.

a. In order to achieve superior intelligence and, in turn, information dominance, the Army must be capable of assimilating the vast sphere of multimedia information, particularly OSI. The rate of change in the number and types of open source databases and network has increased exponentially, resulting in "information overload." Availability and dissemination of information is rapidly expanding on the Internet with a new network coming on-line every 20 minutes. Finally, as the Intelligence Community (IC) and Army continue to downsize, the Army will need to identify and decide which information needs across the spectrum of conflict can best be provided by industry and/or academia to meet real-time requirements within the ever-shrinking decision cycles of military operators and policymakers. Shrinking resources require a focused approach to reduce redundancy and duplication.

b. OSI is an important contributor to contingency planning for conventional and unconventional operations, especially in countries that are not normally peacetime priorities for intelligence collection and production before a crisis. While some OSI loses significance in fast-breaking, high-intensity operations, it regains significance in post-contingency operations. In the case of military operations other than war (MOOTW), validated OSI may become the only intelligence source until classified collection means can be refocused and cued by OSINT. On occasion, it may be the only source needed. If properly focused, OSINT may negate the need to turn to classified “INTS” at all. Low intensity/priority items cannot compete for scarce collection resources and, at times, OSI may be the only source of

intelligence that can fill the specific requirements of a particular topical interest. A focused OSINT approach can provide an invaluable foundation for the spectrum of operational and R&D information needs.

1.3 **OSI Roadmaps**.

a. OSI roadmaps identify the potential sources of information available on or in a target country or mission area. They are particularly pertinent to OSI acquisition through the Internet where they identify relevant uniform resource locators (URLs) and such details as the general content of information found at each source, an assessment of its general level of accuracy, and the timeliness of data normally found at each site.

b. The need for OSI roadmaps to develop information on a specific topic or target area of interest is obvious in this information revolution era. The roadmap establishes directions for OSINT acquisition processing and dissemination of evaluated information on specific Army and IC topics of interest. Roadmaps become particularly important when planning for international political and/or military crises. Crises do not always occur overnight and are normally known days to weeks to months in advance. They can be better prepared for by developing IC/industry/academic/private expert crisis teams well in advance so that all available sources of information and expertise are exploited.

1.4 **Doctrine**.

a. Doctrinally, OSINT should be incorporated into the intelligence process at all levels of command across the full range of operations. Like the other "INTs", with its high volume of data collected, OSINT must process, determine relevance, and protect against vulnerability to deception. Its entry into the intelligence cycle starts with either the analyst who is receiving, evaluating, validating and incorporating it into the final product or concurrently with the collection manager who is knowledgeable of the commander's requirements, mission, and intelligence gaps and acquires what is needed to satisfy these requirements.

b. The use of OSINT in Information Operations (IO) will occur long before a shot is fired, and future success in combat is likely to rely on IO campaigns. Further, information dominance in some future scenarios may allow us to prevail without resorting to military force.

1.5 **Future Prognosis**.

a. The 2010 World is one where most states in all regions, including fewer "denied areas" or "pariahs", engage the rest of the world in the Global Information Infrastructure (GII) and other media arenas to try to win a (virtual) place at the political, economic, and cultural tables of the global community. There will be more information from these countries, their social sectors, economies, private organizations and industries generated in the media and on the World Wide Web (WWW) or its successor. The intent will be to influence, educate, convince, and compete. Sub-national groupings will take advantage in much the same way as nation-states.

b. Much of the OSINT needed by Army and IC customers will be available publicly, internationally or commercially and beyond the origin or control of the US Government. Commercial information industries will be well equipped to process larger amounts of publicly and internationally available data, particularly in digital formats, multi-media presentations, and multi-languages.

c. The Army and IC will have opportunities, if not an imperative, to outsource OSI acquisition and some significant OSI research activities, enabling a smaller government to operate more economically. Outsourcing will enable the government to continue leveraging the cutting edge of the market-driven information industry. Government will still lag several steps behind because of bureaucratic and budgetary inertia.

d. Commercial information industries in all regions will develop products and vie for the global audience beyond their local populations -- for immediate profit and to position themselves for the long-term in the information age competition. It's a marathon, not a sprint. This market will be volatile -- lots of choice for consumers but *the best information will not come inexpensively.*

1.6. **Conclusion**. Forging government partnerships with industry and academia should contribute to developing and sustaining needed OSINT content and identifying the "best of breeds" in emerging information technologies. Their timely insertion into Army and IC OSINT programs, and subsequent evaluation, should contribute to establishing broader based OSI strategies and exploitation capabilities. Government, with business and academia, must seize this window of opportunity for *leveraging* the dynamic global information environment into *innovative, real-time knowledge bases* to maintain its competitive edge in global economics, technology, and information dominance. To be successful, Army OSINT requires dedicated staff and funding.

2.0 OPEN SOURCE INTELLIGENCE (OSINT)

2.1. **Definitions**.

a. Open source 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.

b. Open Source Information (OSI) is comprised of data that is generally distilled by an editorial process that provides some filtering and validation as well as presentation management. These would include for example, widely disseminated newspapers, books, TV and radio broadcasts, and some Internet offerings. The IC further defines Open Source Information as publicly available information (i.e., any member of the public could lawfully obtain the information by request or observation) as well as other unclassified information that has limited public distribution or access. See **ANNEX A** for what is available in the Global Information Environment (GIE).

c. Gray Literature is a subset of OSI. The IC defines Gray Literature as unclassified but less common material which is produced at all levels of government, academia, business, and industry in print and electronic formats, usually available through specialized channels or systems of publication, distribution, and bibliographic control. It is not obtained through normal subscription channels or traditional bookstores to which most people would have ready access.

d. Foreign Public Information Media includes foreign public radio and television broadcasts, foreign press services, foreign publications, foreign Internet sites, and gray literature.

e. Open Source Intelligence (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. See **ANNEX B** for acronym identification and definition of other terms used in this manual.

2.2. **21st Century Information Operations**.

a. OSINT is an essential foundation 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 geo-spatial 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 Counterintelligence (CI), and to Operations Security (OPSEC).

b. OSINT is not a substitute for satellites, spies, or existing organic military and civilian intelligence capabilities. But, it is an essential information source for planning and executing US Army, Joint and Coalition operations across the political-military spectrum. OSINT provides strategic historical and cultural insights of an operational area, including critical information about an adversary's infrastructure and current conditions. It provides vital commercial and geo-spatial information that is not available from national collection capabilities. In coalition operations, OSINT is a foundation for civil-military operations and for cooperation in developing a framework for classified bilateral intelligence sharing,

c. OSINT incorporates academic, business or journalistic research into a stand-alone product or it can be fused with classified sources with the objective of providing all-source intelligence for the commander. In coalition operations, OSINT simultaneously provides a multi-lateral foundation for establishing a common view of the shared area of operations and context for a wide variety of bilateral classified intelligence sharing arrangements.

d. OSINT is valuable to the Army and to Coalition member nations in that it can be used to provide a common understanding of the Area of Responsibility (AOR) 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, civil affairs, 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 (i.e. NGOs), but who are also not authorized access to classified information, can receive tailored OSINT that is helpful to a shared understanding of the AOR.

e. What is new about OSINT is the **confluence of three distinct trends**: first, the proliferation of the Internet as a tool for gathering, 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, such as the former Soviet Union.

f. OSINT is important to Army, Joint and Coalition commanders and their staffs for another reason: emerging threats, and the lower end of the spectrum of conflict, increasing demand of 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 along the EUCOM, CENTCOM, SOUTHCOM and PACOM periphery are all characterized by complex information needs related to infrastructure, demographics, health, and other matters not traditionally addressed by classified intelligence collection operations.

g. OSINT is vital to civil-military operations, and especially to coalition operations, for one additional reason: the changing nature of command and control in the 21" Century. Today, as NGOs 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 and control and information have changed.

h. 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 Coalition troop contributing nations. Under these circumstances, a common view of the AOR formed with the help of validated OSINT is often the most effective means of delivering decision-support.

i. The remainder of this manual will discuss private and government sector information offerings, the open source intelligence cycle, and the integration of OSINT into INSCOM and its MSC operations.

3.0 PRIVATE AND GOVERNMENT SECTOR INFORMATION OFFERINGS

3.1 **OSINT Strategy Fundamentals**.

a. The four pillars to an OSINT strategy are sources, services, analysis and software. 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 INSCOM intelligence staffs.

b. This chapter is intended to expose the reader to a range of OSINT-related products and services that the private and government sector is optimized to provide.

3.2. **OSINT Sources.**

a. 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.

b. While not private sector, two key government information providers, the **US 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.

c. Internet. Since 1995, the Internet has 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.

(1) 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 geo-spatial 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 the Army, Joint Staff and Coalition operators, logisticians, and intelligence professionals.

(2) While the Internet has grown substantially in value since 1995, 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.

(3) The Internet is an "easy information reconnaissance tool" 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. 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.

(4) 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.

(5) In general, the Internet today provides two benefits to the intelligence 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.

d. Commercial Online Premium Sources

(1) There are numerous commercial online premium sources that charge either a subscription fee or a usage fee for their information. It is essential that every professional understand their availability and that decades worth of editorial selection, authentication, formatting, indexing, abstracting, and presentation management went into their information source and database development.

(a) 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. Below, we discuss some of the best known to governments and corporations. There are many others, some unique to Europe or Asia.

(b) Each analyst is urged to consult their librarian or OSINT collection manager to gain a better understanding of what options are available for high-quality commercial information relevant to their information needs.

(c) Because of the high cost of mistakes or unnecessary retrievals commercial on-line 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.

(2) Alacra Inc: http://www.alacra.com

Formerly known as Data Downlink Corp., Alacra Inc. is a privately held global provider of business and financial information. The company's portfolio of service offerings includes the business search engine Portal B and its premium database service .xls. Alacra, Inc. has announced that Mergerstat, a leading supplier of US mergers and acquisitions (M&A) data, will provide Alacra with U.K. and European M&A information.

(3) Chemical Abstracts Service: http://www.cas.org/

Chemical Abstracts Service (CAS) is a division of the American Chemical Society. It is located in Columbus, Ohio. CAS is the producer of the largest and most comprehensive databases of chemical information. Our principal databases are Chemical Abstracts (CA) which contains over 21 million document records from the chemical journal and patent literature, and Registry which contains over 21 million substance and 25 million sequence records. CAS also operates the STN International online service with partner organizations in Europe and Asia. STN provides access to nearly 200 databases covering topics such as science, technology, patents, and business information.

(4) DIALOG: http://www.dialog.com

DIALOG is a very large collection of various commercial offerings that can be searched "by the file." It is 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, actual cost, or pay as you go credit card pricing).

(5) FACTIVA: http://www.factiva.com

FACTIVA has a good web-based user interface and easy 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. It does not include FBIS information. (Flat fee or actual cost pricing).

(6) Hoover's, Inc. http://www.hoovers.com

Hoover's, Inc. delivers comprehensive company, industry, and market intelligence that drive business growth. Hoover's Online Web Site has more than 80-members on its editorial staff that deliver continuously updated intelligence on public and private companies worldwide. Hoover's also delivers its information through corporate intranets and distribution agreements with licensees as well as via Hoover's-branded print and CD-

ROM products. Hoover's is headquartered in Austin, TX, and has offices in New York City and San Francisco.

(7) Jane's Information Group: http://www.janes.com/

Jane's is highly regarded as one of the ultimate sources for defense, aerospace and transportation information. Widely recognized as the publishers of *Jane's Defense Weekly, Jane's Fighting Ships and Jane's All the World's Aircraft*, the Jane's product line includes weekly, monthly, quarterly and annual information products with almost 200 releases in varied frequency and media in any given year. Some of its products are available via the IC OSIS and other Intelink networks.

(8) LEXIS-NEXIS: http://www.lexis-nexis.com

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 ability to reach back several years or more on any topic. (Flat fee, actual cost, or pay as you go credit card pricing).

(9) Oxford Analytica: http://www.oxan.com/

Founded in 1975, Oxford Analytica is an international consulting firm which provides business and political leaders with timely and authoritative analysis of worldwide political, economic and social developments. Oxford Analytica acts as a bridge between the world of ideas and the world of enterprise. One of its major assets is an extensive international network which draws on the scholarship and expertise of over 1,000 senior members at Oxford and other leading universities around the world, as well as think-tanks and institutes of international standing. Some of its products are available via the IC OSIS network.

(10) ProQuest® Online Information: http://www.umi.com/proquest/

The ProQuest® online information service provides access to thousands of current periodicals and newspapers, many updated daily and containing full-text articles from 1986. ProQuest's deep backfiles of archival material are also expanding daily as they digitize 5.5 billion pages from their distinguished microfilm collection.

(11) Questel•Orbit: http://www.questel.orbit.com/

Questel•Orbit aims to provide the most comprehensive and accurate patent, trademark and domain name information. For more than 25 years, Questel•Orbit has been helping manage the world's most important IP portfolios. They provide a suite of leading-edge patent and trademark services to executives, scientists, researchers and competitive intelligence professionals to help turn their information into real value and enhance their organizations' competitiveness. Questel•Orbit services include access to

the world's largest collection of patent information, search tools, digital patent copies and offline expert search services.

(12) Washington Researchers: http://www.washingtonresearchers.com/

Founded in 1974, Washington Researchers has been an acknowledged leader in business and competitive intelligence research for over twenty-five years. Washington Researchers provide in-depth, on-point information about competitors and markets that are not available through "ordinary" print or secondary sources. Washington Researchers' work has been cited by hundreds of publications worldwide, including *The Wall Street Journal*, *Business Week*, and *The New York Times*. They also provide public and private seminars on competitive intelligence techniques, business research, including guides and directories.

(13) The Federation of American Scientists (FAS): http://www.fas.org/

FAS is a nonprofit, tax-exempt, 501c3 organization founded in 1945 as the Federation of Atomic Scientists. FAS founders were members of the Manhattan Project that created the atom bomb and are deeply concerned about the implications of its use for the future of humankind. **FAS** combines the scholarly resources of its member scientists and informed citizens with knowledge of practical politics. FAS is uniquely qualified to bring the scientific perspective to public policy and provides advocacy papers and briefings for policy makers, the press, and the public. Its in-depth index on military, S&T, and related topics provide an excellent first stop reference site on these subjects.

e. Information Brokers

(1) Information Brokering describes the services of information professionals or information research consultants worldwide, who perform online searching, library research, competitor intelligence, and similar services for business, industry, government, academia and the scientific communities. These knowledge workers charge for their expertise at locating, analyzing and/or interpreting information for use by a client. Most subscribe to the principles contained in the Codes of Ethics of organizations like the Association of Independent Information Professionals (AIIP), the European Information Researchers Network (EIRENE), the Public Record Retrievers Network (PRRN), and the Society for Competitor Intelligence Professionals (SCIP). Competitive intelligence professionals are expert at collecting, analyzing and disseminating information in a timely manner that allows decision makers in an organization to achieve a competitive advantage.

(2) Most professional information brokers, such as those belonging to the Association of Independent Information Brokers (AIIB) at http://www.aiip.org/, specialize in selected databases like LEXIS-NEXIS or DIALOG. Another group that specializes in OSINT is the Society of Competitive Intelligence Professionals at http://www.scip.org.

(3) The Burwell Directory of Information Brokers (Burwell Enterprises, Dallas, TX; http://www.burwellinc.com) is an annual directory which also indexes all brokers according to their specific areas of expertise (e.g. electric power, POL industries, transportation, etc.) their range of database access, and, their mastery of foreign languages and foreign databases. It is now possible to obtain the services of a SME who is both a linguist and familiar with the databases in countries where that language is spoken.

(4) There are distinct advantages in contracting a searcher who has detailed familiarity with the Internet and the very arcane search command characteristics of commercial database 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. Always ask for search results in electronic form. These files can more easily be shared and placed into an all-source database.

f. 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. A few sources of common interest to military commanders and their staff can be viewed in **ANNEX C**.

g. Gray Literature

(1) Gray literature is unclassified information which is produced at all levels of government, academia, business, and industry in print and electronic formats, usually available through specialized channels or systems of publication, distribution, or bibliographic control. Gray literature is not obtained through normal subscription channels or traditional bookstores to which most people would have ready access. Gray literature includes marketing materials from trade shows and exhibitions, white papers, conference proceedings, trade and business directories, working papers, trip reports, pre-prints, technical reports and technical standards documents, dissertations, data sets, and commercial imagery. Gray literature cuts across scientific, political, socio-economic, and military disciplines.

(2) Producers of gray literature include: national and foreign government ministries, academia, research institutes, think tanks, nonprofit and educational organizations; commercial enterprises creating documents for internal use as well as for clients and suppliers, trade associations and unions, local and state 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.

h. Overt Human Experts and Observers

(1) 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.

(2) 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 will be less reliable than direct human expert judgment or observation.

(3) There are essentially four ways to get human expertise.

(a) 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 http://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.

(b) The second means is through professional associations such as those listed in the "International Directory of Associations" published by Gale Research, or as found through a http://copcmic.com search of the Internet.

(c) The third means is by doing a Factiva.com search and identifying experts that have been quoted in the media on that topic.

(d) 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.

(4) 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 as in-house points of contact.

i. Commercial Imagery

(1) The commercial imagery industry continues to mature with the launching of a number of satellites that offer militarily significant capabilities. One-meter resolution electro-optical imagery is already available to the private sector and has very useful military applications. By the end of 2003, several more private companies are expected to have high-resolution commercial remote sensing satellites in orbit. Their products will be available to whoever has a credit card.

(2) While this will bring new capabilities to friend and foe alike, commercial imagery provides unique opportunities for Coalition use as well. Unbridled by security

constraints, which limit the use of imagery derived from military satellites, commercial imagery acquired by Coalition forces 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 will not have access to classified information.

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

(4) 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.

(5) 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 Coalition forces as well as to our adversaries.

(6) A number of Coalition nations purchase commercial imagery to support their own national imagery requirements. In many cases, these images can be redistributed freely. While Coalition 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.

(7) 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.

(8) Commercial satellite imagery is adequate to assist in developing the following targets: troop units, vehicles, aircraft, airfield facilities, nuclear weapons components, missile sites, rockets and artillery, surface ships, surfaced submarines, roads bridges, radar and radio sites, command and control headquarters, supply dumps, land minefields, urban area strategic sites, landing beaches, ports and harbors, railroad facilities, and key terrain.

j. Other US Government, Coalition and Non-Govenment OSINT sources include, but are not restricted to:

(1) Intelligence Community (IC) organizations are not responsible for satisfying the commander's specific needs for OSINT, but they may have relevant open source information that can be provided. The IC Open Source Information System (OSIS) provides readily available information but it is dated in some instances. Future OSIS expansion of the network to include Homeland Security needs and purchase of additional commercial open source content will enhance its utility to OSINT users.

(2) Army Foreign Military Studies Office (FMSO). FMSO is a TRADOC organization and has exceptional research credentials, databases, and some linguistic capability for doing original translation of open source material. FMSO researches, writes and publishes from unclassified sources about the military establishments, doctrines and strategic, operational and tactical practices of selected foreign armed forces. It also studies a variety of civil-military and transnational security issues affecting the US military, such as peacekeeping and peace enforcement, counter-drug support, terrorism, insurgency and peacetime contingency operations. FMSO's studies, articles, briefings and lectures broaden understanding of foreign military developments and support policy formulation, decision-making and military education. FMSO actively participates in military-to-military and academic outreach programs with the commonwealth of Independent States and other countries around the world. FMSO is augmented by Reserve Component personnel and maintains an IC online database keyed to specific requirements called the World Basic Information Library (WBIL). http://fmso.leavenworth.army.mil/

(3) The Asian Studies Detachment (ASD) is a subordinate element of the Army's 500th MI Group and is one of the Army's premier OSINT producers. The ASD exploits open source information from over 650 regional publications and electronic sources, most published in the vernacular, in support of US Army Pacific intelligence requirements. ASD is unique in that most of the organization is comprised of Japanese civilians, many with extensive military experience. ASD's open source exploitation is published as Intelligence Information Reports (IIRs) under its unique reporter code.

(4) The Virtual Information Center (VIC) provides the US Commander- in-Chief Pacific with situational awareness, a fused picture, not something possible through traditional methods. They accomplish this through the timely and focused identification, retrieval, integration and analysis of open source information by advanced technology and information. VIC was conceived in 1997 as an open source information network, operating outside of the traditional intelligence and operational information box that would facilitate timely delivery of crisis-driven information to decision makers. The VIC specializes in geopolitical analysis of the major events in the Asia Pacific Region and maintains an extensive country database of Websites. http://www.vic-info.org

(5) Library of Congress/Federal Research Division (LOC/FRD). FRD is the Library of Congress's principal fee-based research and analytical service. Its mission is to

provide directed research and analytical products on a wide range of social and physical science topics to agencies of the United States Government, authorized Federal contractors, and agencies of the government of the District of Columbia. FRD uses Library of Congress collections and staff expertise to exploit these and other information resources worldwide. FRD can translate from 25 foreign languages into English and also offers selected translation services from English into a variety of foreign languages. http://www.loc.gov/rr/frd

(6) Defense Technical Information Center (DTIC). DTIC is the central facility for the collection and dissemination of scientific and technical information for the Department of Defense (DoD). Much of this information is made available by DTIC in the form of technical reports about completed research, and research summaries of ongoing research. DTIC manages 13 Information Analysis Centers staffed by experienced information specialists, scientists and engineers who help customers locate, analyze and use scientific and technical information in a specialized subject area. DTIC's use of leading edge technology allows customized information to be gathered at rapid speeds and deployed to its customers using state-of-the-art communications. To utilize DTIC's products and services you must be a registered user. http://www.dtic.mil

(7) Some Coalition Partners such as NATO and its respective members like The Netherlands, United Kingdom, Denmark and Norway, are exceptionally competent in the OSINT area and have fully integrated OSINT into their all-source collection and production environments.

(a) Established Coalition and US diplomatic missions and those of various Coalition members 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.

(b) Many of the Coalition members have Chambers of Commerce and these often have 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.

(8) Non-Governmental Organizations (NGOs) like 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.

(9) Many Religious Organizations 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.

3.3. **Defining Source Access Requirements**.

a. It is a relatively easy endeavor to identify private information sources that can support the information needs of an OSINT program. 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 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.

b. 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.

c. 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.

4.0 THE OPEN SOURCE INTELLIGENCE CYCLE

4.1. **OSINT Planning and Direction**.

a. 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. 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.

b. Since many Requests For Information (RFIs) 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 Army and Coalition planning and operations. While OSINT is an emerging discipline, emphasis must be placed on the OSINT Process fundamentals:

(1) Discovery - Know Who Knows

(2) Discrimination - Know What's What

(3) Distillation - Know What's Hot

(4) Dissemination - Know Who's Who

4.2. **Organizations and Responsibilities**.

a. The Land Component Commander (LCC) 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.

b. The subordinate MSC commanders for Civil Affairs, Public Relations, Military Police, and Combat Engineering units may often be the best channels for seeking out MSC related OSINT data.

4.3. **Requirements Definition**.

a. 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.

b. 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.

c. OSINT is the most fundamental and fastest means of satisfying basic informational needs, including needs for historical background, current context and general geo-spatial 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.

4.4. **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.

4.5. **Processing Services.**

a. Processing services include data conversion from hardcopy or analog to digital, indexing and abstracting of hardcopy or softcopy textual data or images, interpretation and annotation of imagery or signals, database construction and stuffing, and complex modeling and simulation projects with the best ones including geo-spatial and time-based visualizations.

b. 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. See **ANNEX D** for an initial list of private processing services.

4.6. **Analysis and Production Services.**

a. 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.

b. 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. However, 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.

c. 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.

d. Web-site analysis is another tool, which can be applied to vet the capabilities of a potential information vendor. 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.

4.7. **Evaluation and Feedback**.

a. 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.

b. 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.

5.0 OSINT COLLECTION

5.1. **OSINT Collection Management**.

a. 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 most accurately answers a valid need. Once an intelligence need has been identified, open sources should be reviewed by the OSINT Team to determine if that need can be satisfied through OSINT. Other things to be considered are organic collection assets and/or those of higher command or IC control or if an RFI to Coalition partner is required, or if a combination of these approaches is required.

b. Collection requires the translation of an information need into an intelligence requirement and 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.

c. In the INSCOM 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.

d. Requests For Information (RFIs) from intelligence users typically generate collection efforts. The four types of OSINT generated intelligence collection and production requirements are: 1) analyst driven, 2) events driven, 3) commander/operator driven and 4) target/database update driven.

e. The four categories above outline the way in which an internally directed OSINT 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.

f. 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.

g. An analyst is often best placed to determine what product is required to address the past needs of the intelligence user. Proactive collection management makes effective use of emerging information and 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.

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

i. 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.

j. Chapter 2 reviewed private and government sector information offerings. Chapter 3 focused on the OSINT intelligence cycle and methods to be applied to exploit those offerings. What is important is that every analyst and collection manager 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. **ANNEX E** provides a high-level view of the elements of the OSINT process.

5.2. **Knowing Who Knows**.

a. During periods of stability as well as crisis, it is incumbent upon the INSCOM Staff to establish and nurture sources that will help satisfy information requirements. It is vital that the OSINT Team 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.

b. An approach favored 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.

c. 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 IC, government departments, Coalition partners, and into the 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.

d. The command OSINT Team is, in essence, an information LNO 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 Army concerns with regard to OPSEC.

5.3. **Collection Discipline**.

a. There is no faster way for an OSINT staff officer 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.

b. 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 OSINT Team should closely manage the efforts of OSINT contract collectors to ensure that OSI is timely inserted into the all-source process.

c. A suggested timetable or “rule of thumb” for a routine, non-complex Internet OSINT RFI is provided below:

RFI Definition:	Ensure an understanding of commanders. Intent.	30 Min
Internet Collection:	Use search tools, rapidly identify top ten sites and review.	30 Min
Internet Bookmark:	Create Internet Bookmarks for future use and for customer's reference.	15 Min
Commercial Collection	Use fee sources, identify top 20 items for exploitation.	60Min
Analysis:	Read, understand, evaluate, and structure collected information	120Min
Production:	Carefully create an analytical summary, table of contents, and slides.	60 Min
Total time required to answer an Internet OSINT RFI using only internal resources:		**5 Hrs, 15 Min**

d. The desire to continue with the 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 open source collection, "*pursuit of perfection is the enemy of good enough*."

e. 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 can exploit for specific issues. This reference aid will serve as the starting point for subsequent analytical tasks.

5.4. **Collection Issues**

a. 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.

(1) Operations Security

(a) OPSEC is easily achievable in the OSINT environment through four measures. First, the concealment of the origin of the search through the use of trusted intermediaries (i.e. contractors); second, using good Internet Security practices (see **ANNEX F)**; third, using approved non-attributable Internet access; and fourth, the utilization of normal commercial Non-Disclosure Agreements (NDA) when necessary to protect direct discussions of a commander's concerns and intentions.

(b) 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.

(c) The private sector is accustomed to protecting proprietary and commercially confidential discussions. A standard private sector NDA is a good privacy agreement, with the added advantage that the private sector partner has a financial motivation for honoring the NDA if they want more business. Discretion is part of what they are selling.

(2) Intellectual Property Rights Compliance

(a) Intellectual property rights (e.g., copyright, trademark, and patents) must be respected. Exceptions based on urgent mission needs must seek approval of the Intellectual Property Counsel of the Army (IPCA). An infringement approved by IPCA will not insulate the command using the work from subsequent liability for the costs of infringement.

(b) 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 essential for INSCOM and its MSCs to learn how

to properly comply with applicable copyright provisions. This is important for two reasons:

(1) To maintain the highest standards of legal and ethical behavior among all INSCOM elements; and

(2) More often than not, OSINT will be shared with external private sector parties (e.g. humanitarian assistance organizations) or used as a means of Coalition partner information exchange. Thus copyright compliance is a vital means of maintaining future flexibility in the exploitation of available OSINT.

(c) Information marked with copyright, or other intellectual property restrictions will be appropriately cited when used. Refer to the SJA for questions pertaining to copyright and property rights.

(3) Foreign Language Shortfalls

(a) Despite the multi-cultural and multilingual nature of existing alliances, many contingencies require foreign language skills that are not readily available within the Army, DOD or IC. Linguists cannot be identified quickly and provided with security clearances.

(b) 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 INSCOM/IDC Intelligence Architecture plan. Foreign language technology "triage applications" need to be incorporated into the plan as soon as feasible.

(c) Understanding international terrorism, insurgency, and violent internal political opposition movements requires competency in a number of foreign languages. While some of the required language capabilities are within the competence of DOD/IC intelligence organizations, these capabilities are unlikely to be made available to Army commands for the exploitation of OSINT.

(4) External Networking

(a) There are four obstacles to external networking relevant to Army competency in OSINT.

(1) There is a lack of knowledge about who the real experts are on various regional and topical issues.

(2) There is a fear of revealing the RFI question as an official inquiry. Procedures for dealing with or making direct contacts between intelligence personnel and private sector experts need to be developed.

(3) There is the lack of funding for compensating subject-matter experts.

(4) Finally, existing command and control, communications, computing, and intelligence (C4 I) architectures prohibit routine access to the Internet, and often make it difficult if not impossible to migrate unclassified information from the Internet into classified databases.

(b) The technology is available but current DIA policy does not provide parameters or procedures for accomplishing this capability. All of these obstacles can be overcome with Command Element support.

5.5. **Reserve Component (RC) OSINT Contribution**.

a. The use of Army and other Service RC assets in the gathering, processing, translating and analysis of OSI needs to be established early. Once operating procedures and memorandums of understanding are formalized, RC individuals or units can be focused on "data mining" of the public Internet and related sources in support of General Military Intelligence (GMI), S&T and force developer information requirements.

b. INSCOM can acquire IC OSIS User IDs and Passwords for RC individuals or elements from the Community Open Source Program (COSP) to facilitate accessing, searching, acquiring, processing, distributing and manipulating OSINT for INSCOM MSCs.

5.6. **Outsourcing as a Partial Solution**.

a. Commercial vendors, universities, and military reservists have the background and experience to accomplish the continuous data monitoring and acquisition task in a responsive manner that supports IC transnational, MOOTW, and MRC issues. Industry and academic centers have information specialists with expertise on various regions of the world and subject areas. These non-government analysts can acquire and pre-process OSI that will help satisfy many civil, political, law enforcement, economic, and military community information requirements.

b. US responsiveness to natural and manmade disasters relies heavily on a variety of open sources, especially information provided by humanitarian relief organizations. OSI from previous or existing IC external research contracts on a country's or region's national cultures (religions, customs), personalities, and basic infrastructures (food, water, medical, communications, transportation, critical supplies, power generation, and distribution systems) is invaluable in obtaining a realistic "picture" of the crisis and taking appropriate action.

c. Two objectives for meeting the needs of policy makers and commanders will be satisfied when incorporating OSI vendors into the flow of intelligence.

(1) Fulfill short-suspense contingency requirements through accessing, filtering, and maintaining on-call source data.

(2) Provide strategic-level open source research to alert the Intelligence Community about activities that indicate abnormal or potentially alarming situations

d. A thorough understanding of available and useful sources of information is essential in meeting OSI research requirements. Many commercial vendors, academics, and reservists maintain their current knowledge of the GIE by holding membership in professional organizations dedicated to information research. They network and attend professional, international symposiums, conventions, and trade shows to keep abreast of new avenues of OSI and to pursue commercial business interests. In addition, these information specialists have built both domestic and international networks of academic and professional contacts that can be leveraged.

e. Industry and university centers maintain contemporary technical libraries with topical reference books, specialized publications, and journals from around the world. They rigorously evaluate sources of information to minimize bias and unsubstantiated facts that may have been reported or published. These OSI providers also acquire information not readily available through data services, soliciting information from non-electronic sources such as embassies, trade missions, and foreign libraries and organizations.

e. Because focused data acquisition is a fundamental part of their business, these OSI providers are experienced at acquiring gray literature (publicly available information that is not distributed through normal publishing channels). Examples of gray literature are academic writings, conference proceedings and trade show literature, video and still imagery reports, marketing research studies, international tender documents, and industry-sponsored research. Knowing what information is available and obtaining it requires a staff experienced in nontraditional research methods with a broad base of commercial contacts.

5.7. **Selection of OSI Vendors, Academia, and Reservists.**

a. A prospective OSI vendor or reservist supporting the IC should have extensive experience and understanding of the intelligence arena, various regions of the world, and specific topical expertise pertinent to customer needs. These organizations or individuals should have access to trained information specialists and/or intelligence analysts with a wide range of experience in applications software.

b. Individuals must keep current with new developments in database applications, information retrieval methods, fusion, validation of information, and collection. Small, high-quality consultant teams and/or larger vendors should be able to present a list of experts and specific skills available to fulfill tasks.

5.8. **OSI Statement of Work (SOW) Considerations.**

The following are some of the questions that need to be addressed in developing a Statement of Work (SOW) before employing a vendor in executing an OSI pilot project:

a. Which non-IC resources can potentially address this problem?

(1) Other DOD/government research and analysis organizations that are not part of the IC

(a) Corporate researchers and market analysts
(b) Academic researchers
(c) Other non-government researchers

b. Reserve/National Guard intelligence units and individual mobilization augmentees (IMAs)

c. How will information providers be selected? What are the evaluation criteria for selection?

d. How will information providers be tasked?

e. How will information providers be compensated? Retainer? By the hour? By the finished product?

f. How is the value versus cost of these products assessed?

g. What are the deliverables, timeframes, and costs?

h. How are finished products delivered (hardcopy, hypertext markup language (html), multimedia, etc.) and disseminated for use by IC analysts?

i. What measurement criteria and other evaluation mechanisms will be specified in advance?

5.9. **Collection Nuances.**

a. The Internet, despite its current and projected growth, is primarily a vehicle for OSINT reconnaissance and collaboration, rather than a complete repository of knowledge. It will never be a completely trustworthy source for information. The Internet also is not a substitute for premium fee-for-service commercial online databases, and it is vital that no Army element falls prey to this illusion.

b. Internet search engines, even recommended meta-search engines, have severe limitations. By some accounts, any 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 that do not allow access by routine search engines. While many sites are free and some are available by subscription, search engines are simply ineffective.

c. Some Internet software tools like Lexibot can assist in collection from the "deep web," but considerable collection time can be expended in obtaining relevant information. For this reason, skilled OSINT contractors should be employed to acquire this data and they should provide the government the "Cybersearch URL Catalogs" along with appropriate notes on the value of the various sources used.

d. These URL Catalogs with notes allows the sorting of 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 INSCOM MSCs cooperate and share URL Catalogs with each other, a very comprehensive directory of web resources should emerge.

e. As the Army deals with more non-traditional threats and worldwide stability scenarios, OSINT will become a critical element of the all-source intelligence process. It is vital that every MSC commander and relevant staff member begin now to understand and plan for OSINT needs.

f. Training in open source exploitation is relevant not only to the intelligence analysts and collection managers, but also to all relevant staff members who need access to OSI. OSINT is not the exclusive purview of the intelligence profession. Intelligence staffs should enable all staff elements to access relevant open sources as directly as possible.

g. 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 program can reduce the number of unnecessary RFIs that bog-down the all-source intelligence staff with information requests that can otherwise be satisfied.

h. 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 and staff operations.

i. 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.

j. Gray 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 INSCOM OSINT process should include the inventory and evaluation of

gray literature sources, and the development of a strategy, a budget, and a process for assuring that gray literature sources are fully integrated into the INSCOM/IDC future intelligence architecture.

6.0 OSINT PROCESSING AND EXPLOITATION

6.1. **Overview**.

a. While "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 is a critical step.

b. 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. Since much of OSINT is not in digital form, hands-on human translation and evaluation are the most important part of processing and exploitation.

6.2. **Tools**.

a. In order to maximize use of the Internet and process the exponential volume of OSI, advanced pre-processing and exploitation tools will be required to meet the challenge. Pre-processing tools are needed to screen, find, capture, compile, extract, index and prepare the data for analysis. Exploitation tools are needed to search, retrieve, manipulate, and display the pre-analyzed data in advanced ways, using techniques such as visualization to aid in understanding. OSINT managers should remain abreast of developments in analysis tools, and integrate them, as they become available, into their OSINT process.

b. Without a dedicated set of automation tools, OSINT production will continue to be reliant upon ad hoc software solutions and arduous analytical effort. See **ANNEX G** for available INSCOM application tools.

6.3. **Analysis**.

a. 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. **ANNEX H** provides a list of some common misperceptions and biases.

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

c. 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

d. It is also helpful when processing open source 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.

6.4. **Web-Site Authentication and Source Analysis**.

a. 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 international 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:

(1) Accuracy

(a) 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.

(b) 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.

(2) Credibility & Authority

(a) Does the web-site clearly identify itself? Is there merely an E-mail address or a full name, address and telephone number. Sam Spade at URL (http://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.

(b) 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?

(c) 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.

(d) 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.

(3) 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).

(4) Objectivity

(a) 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.

(b) To whom does the web site link? Many sites provide a list of relevant links. These links 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.

(5) Relevancy

(a) 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.

(b) See **ANNEX I** for a Web site Evaluation Checklist.

6.5. **OSINT Production**.

a. As opposed to other intelligence disciplines, OSINT relies on outward engagement beyond the institutional confines of 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.

b. 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.

(1) Reports

(a) An OSINT report could consist of OSI data collated together for generic interest and wide dissemination or OSINT that has been discovered, discriminated, distilled, and disseminated to a specific consumer in order to answer a specific intelligence need.

(b) OSINT analysts 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.

(c) A report should have an analytical summary. This is the value-added expertise from an analyst who has screened and integrated multiple OSI data into an underlying framework, and then devised an executive summary that can stand on its own.

(d) 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. *It should be noted, however, that the integration and analysis of sensitive open sources could lead to a classified result in some instances.*

(e) By providing the consumer (commander, operator, logistician, or 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.

(f) 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, Gray 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. The OSINT report format follows:

OSINT REPORT

DATE OF INFORMATION: (ddmmyy) (e.g. 26/11/02)

COUNTRY: (e.g. Saudia Arabia)

TITLE:

TOPIC: (e.g. Economy)

ABSTRACT: (Summary of key facts)

ANALYTICAL SUMMARY: (Value added analytic summary)

APPENDED DOCUMENTS: (copies of whatever is extracted from Internet or other sources)

AVAILABLE LINKAGE (s): (key URLs)

ORIGINATOR: Name:
Phone:
Email:

REQUEST FOR INFORMATION (RFI) NUMBER: (if known and applicable)

SOURCE (s):

1 (best of # read sources from # screened sources)
2 (best of # read sources from # screened sources)
3 (best of # read sources from # screened sources)
4 (best of # read sources from # screened sources)

COPYRIGHT: (if applicable or N/A)

CLASSIFICATION: UNCLASSIFIED FOR OFFICIAL USE ONLY

(g) As INSCOM develops its niche in the OSINT arena, an OSINT sub-portal should be developed within its current all-source Command Portal to facilitate collaboration and sharing of OSINT. The US Pacific command initiative known as the Virtual Information Center is a good example of this process. It can be accessed at http://www.vic-info.org.

6.6. **Dissemination and Evaluation**.

a. 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.

b. This makes it extraordinarily valuable in dealing with Coalition partners and civil sectors, including NGOs, that traditionally distrust the military in general and intelligence professionals in particular. As INSCOM continues to evolve and transform

itself in response to the many new challenges, the importance of OSINT will continue to evolve.

c. Once open source information has been developed into OSINT, it can be disseminated via any of the IC Intelink networks. At a minimum, it should be placed on the IC OSIS network where it can be easily shared with other IC members and placed on SIPRNET so that it can be easily integrated into the all-source process. If the OSINT product has value to other parts of the Army community, it should also be placed on the Army Knowledge On-Line (AKO) network. Once on any of the above networks, it can be placed in a "push" mode, or it can be "pulled" off on demand.

d. 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.

e. The approach should be flexible to fully leverage the ability of OSINT products to provide a medium for engaging Coalition partners in security discussions or in the development and dissemination of a common view of the operating area.

6.7. **Summary.**

a. 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.

b. OSINT is even more important in 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.

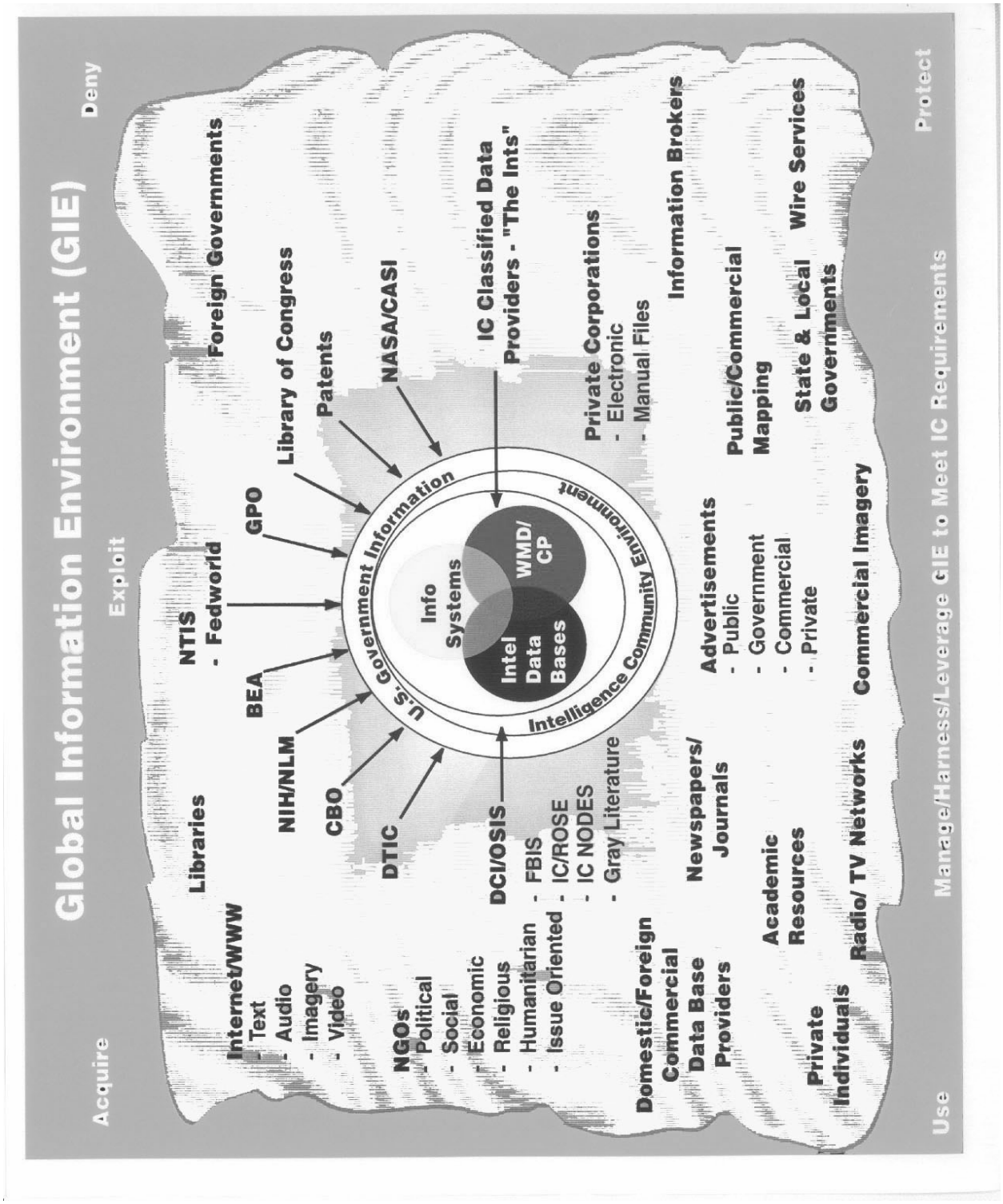
c. OSINT's four main contributions to classified collection are: tip-off for classified sources; targeting of those sources; context and validation to better understand material collected from classified sources, and; providing plausible cover to protect the classified source.

d. The objective of a robust OSINT capability should be to increase the range of information available to intelligence users.

e. A suggested organizational structure to maximize OSINT support to INSCOM’s MSCs, the Army, in general, and its deployed Land Component Commanders (LCC) is an INSCOM OSINT Reach Back Center. A high-level functional structure is provided at ANNEX J.

ANNEX A

Global Information Environment (GIE)



ANNEX B

Glossary

AIIB	Association of Independent Information Brokers
AIIP	Association of Independent Information Professionals
AKO	Army Knowledge Online
AOR	Area of Responsibility
API	Application Program Interfaces
BBC	British Broadcasting Corporation
BEA	Bureau of Economic Analysis and also Bureau of Export Administration (both elements of the Department of Commerce)
CASI	Center for Aerospace Information (NASA)
CBO	Congressional Budget Office
CIA	Central Intelligence Agency
COSPO	Community Open Source Program Office
COTS	Commercial off-the-shelf
DASD	Deputy Assistant Secretary of Defense
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DOD	Department of Defense
DTIC	Defense Technical Information Center
EEI	Essential Elements of Information
EIRENE	European Information Researchers Network
FBIS	Foreign Broadcast Information Service
GIE	Global Information Environment
GII	Global Information Infrastructure
GMI	General Military Intelligence
GOTS	Government off-the-shelf
GPO	Government Printing Office
HTML	Hypertext Markup Language
IC	Intelligence Community
ICRC	International Committee of the Red Cross
IDC	Information Dominance Center

ANNEX B

Glossary
(Cont)

IMA	Individual Mobilization Augmentee (military reservist)
IO	Information Operations
IPCA	Intellectual Property Counsel of the Army
I&S	Intelligence and Security
ISP	Internet Service Providers
LCC	Land Component Commander
LOC/FRD	Library of Congress/Federal Research Division
LNO	Liaison Officer
MARC	Machine-Readable Cataloging
MCCIS	Maritime Command and Control Information System
MIT	Massachusetts Institute of Technology
MOOTW	Military Operations Other Than War
MRC	Major Regional Conflict
MSC	Major Subordinate Command
MT	Machine Translation
NAIC	National Air Intelligence Center (US Air Force)
NASA	National Aeronautics and Space Administration
NATO	North Atlantic Treaty Organization
NDA	Non-Disclosure Agreements
NFIP	National Foreign Intelligence Program
NGO	Non-Governmental Organization
NIH	National Institutes of Health
NIST	National Institute of Science and Technology
NLM	National Library of Medicine
NTIS	National Technical Information Service
OAEP	Open Source Information Acquisition/Exploitation Pilot
OPSEC	Operational Security**OSI** Open Source Information

ANNEX B

Glossary
(Cont)

OSINT	Open Source Intelligence
OSIS	Open Source Information System
PRRN	Public Record Retrievers Network
R&D	Research and Development
RFI	Request for Information
ROSE	Rich Open Source Environment
SAR	Synthetic Aperture Radar
SCI	Science Citation Index
SCIP	Society for Competitor Intelligence Professionals
SME	Subject Matter Expert
SSCI	Social Science Citation Index
STN	Scientific and Technical Network
SOW	Statement of Work
TRADOC	Training and Doctrine Command
UN	United Nations
URL	Uniform Resource Locator
USAF	United States Air Force
VIC	Virtual Information Center
VPN	Virtual Private Network
WMD/CP	Weapons of Mass Destruction/Counterproliferation
WEU	Western European Union
WWW	World Wide Web

ANNEX C

A Selected List of Open Sources

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 Events (Conferences)	British Library Proceedings http://www.bl.uk/services/bsds/dsc/infoserv.html#inside_conf
Current Events (Journals)	ISI Current Contents http://www.isinet.com/
Current Events	Oxford Analytica http://www.oxan.com/
	CNN International http://europe.cnn.com/CNNI/
	Fox News http://www.foxnews.com/
	The Times http://www.thetimes.co.uk/
	LA Times http://www.latimes.com/
	Jerusalem Post http://www.jpost.com/
	The Washington Post http:/twww.washingtonpost.com/
	South China Morning Post http://www.scmp.com/
	The Japan Times http://www.japantimes.co.jp/
	World Newspapers Online http://onlinenewspapers.com
Defense Monitoring	Janes Information Group http://www.janes.com/geopol/geoset.html
Defense Monitoring	Periscope http://periscope1.com

ANNEX C

A Selected List of Open Sources (Cont)

Defense Monitoring (NATO)	Orders of Battle Inc. http://orbat.com
Directories of Experts	Gale Research http://www.gale.com/
Foreign Affairs Monitoring	Columbia Univ. Int'l Affairs Online http://ciaonet.org
Foreign Affairs Monitoring	Country Watch.com http://www.countrywatch.com
Global Risk Monitoring	Political Risk Service (Country Studies) http://www.prsgroup.com
Maps & Charts	East View Cartographic http://www.cartographic.com
	CIA World Factbook **http://www.odci.gov/cia/publications/factbook/docs/refmaps.html**
	United Nations http://www.un.org
	World Maps Online http://www.lib.utexas.edu/maps
Language Translation Online	http://babelfish.altavista.com
Conflict/Natural Disaster Impacts	United Nations High Commission For Refugees http://www.unhcr.org

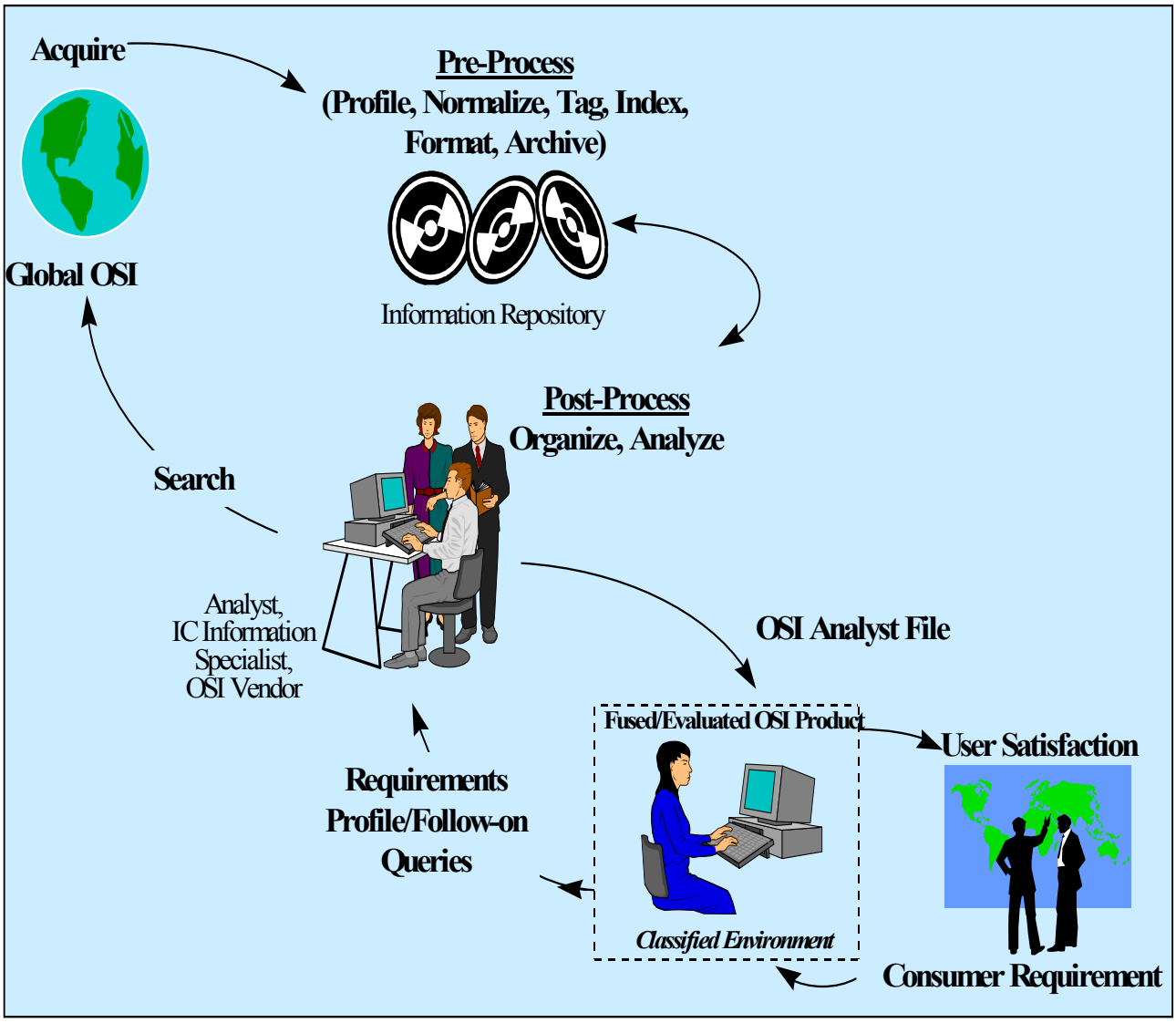
ANNEX D

OSINT Related Service Examples

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

ANNEX E

OSINT Process Overview



ANNEX F

Internet Security Tips

The Internet is a Valuable Source of Information

The Internet is an unparalleled source of breaking news, in-depth information and exhaustive background resources for further research. According to the American Journalism Review's (AJR) NewsLink, in early 2001, there were 5,400 daily newspapers with online editions, with more popping up every day. Almost half of those are published outside the United States.

In addition, there are the major all-news sites, such as ABCNEWS, MSNBC and CNN. Add to that Web based magazines such as Salon, Feed and Slate, plus the online editions of national and international magazines such as The Atlantic Monthly, The Economist and the Far Eastern Economic Review, and you have a major periodical library online. There are also the news roundups on portal sites such as GO or Yahoo, and online news directories such as NewsHub. But online newspapers and magazines are only one way of searching for information online. There's hardly a subject imaginable that does not have its own Web site, complete with links to other resources and comprehensive historical and background material.

Looking for current information on the high-tech industry? The Web is a gold mine of technology news sites, from the encyclopedic ZDNet to the sharp writing of The Industry Standard to the trendy Wired.com.

Need to keep up with events in the former Soviet Union and Eastern Europe? The Soros Foundations Network, linking the multiple open society foundations created by billionaire investor George Soros, is an unparalleled resource for the Newly Independent States and the fledgling democracies of Eastern Europe and Eurasia. Subject areas and associated web sites are endless.

While the information to be sifted is invaluable, there are very important security issues to be considered while surfing the net. There is no hotter issue in cyberspace than the ongoing debate about personal privacy on the Internet.

The Net's wide-open nature and its power to transfer information, make it relatively easy for individuals to find out more about you than you want them to. Web technologies like cookies make your surfing habits available to advertisers. E-commerce sites can track your purchases. Your employer can read your e-mail. The law in many of these instances is still unformed. With the added challenges of the very real possibility of attack by a virus or some other variety of digital-bug, how can you feel safe venturing online? There are a number of precautions you can take to protect yourself and others who share your cyberspace.

ANNEX F

Internet Security Tips

(Cont)

The Wires Have Ears!

Many new Internet users assume they visit Web sites anonymously. They are wrong. When you visit a Web site, you leave behind footprints, both on the Web site and on the computer you use. A recent federally funded study found that 92.8% of all Web sites collect personal information. The invasiveness of the information collected varies.

There are several ways to trace users via the Internet. Here are a few:

1. The IP Address. This is the address used to connect to the Internet.
2. E-mail. Your IP address can also be captured by opening an e-mail that contains a web page (HTML e-mail). If the web page requests a graphics file from a server your IP address, as well as the type of e-mail program you are using, is captured. The web page can also place a cookie on your system that can be used to track you later.

3. Your e-mail address. Normally a user can only be traced back to their Internet Service Provider. Once e-mail reaches an ISP the e-mail is routed internally. Often web-based e-mail accounts (such as Hotmail) display the senders real IP address in the header so a sender's ISP can often be determined even if they use an 'anonymous' account. Another way is just search using the address. Postings, web pages, and other information may be found this way.

4. Loading software. By running an executable program or script, virtually anything can be read from the hard drive. Files could be read, hidden "Trojan horse" programs can be loaded, even programs that allow others to run your computer over the Internet can be installed.

Viruses and Other Illnesses

Viruses, worms and Trojan horses are human-made software programs created specifically to wreak havoc on personal computers and networks. The odds of downloading one of these computer viruses over the Internet have increased dramatically recently. Sometimes a strange message may appear on your screen. In a worst case scenario, all the data on your hard drive may be wiped out. These destructive programs may start out on one computer, but they get replicated quickly and infect other computers around the world.

In 1988 a student at Cornell University sent one out by accident, infecting more than 6,000 computers in minutes, nearly bringing the Internet to its knees. More recently, the

ANNEX F

Internet Security Tips

(Cont)

"I Love You" virus caused over $1 billion in lost productivity as it crippled e-mail systems around the world.

Virus Prevention Guidelines

1. Make sure your computer runs anti-virus software. If not, buy and install it immediately.

2. Even if you have this software, it has to be updated regularly, as new viruses appear daily. Many products have a feature that will automatically download updates, making it easy to stay protected. It is strongly recommended that users download the updates at least once a week to keep your computer as secure as possible.

3. DO NOT OPEN an e-mail attachment unless you know who sent it. Even then, it's not totally safe, as a sneaky virus that has infected a friend's computer can access the e-mail address book, send a message to everyone, and attach itself. To be completely safe, scan the attachment with your anti-virus software before you open it.

4. If you receive a suspicious message, delete it immediately from your In Box. When you delete a message, however, it's still on your system. Go into the Deleted Mail folder and delete the message again to permanently remove it.

5. Regularly back-up your files. Should your system become infected, you won't lose your valuable data. If you download and run software from the Internet, or receive e-mail attachments, there's a good chance of contracting one of these digital bugs. How can you protect yourself? Virus protection programs scan your hard drive for viruses and delete them. The two best known are Norton Anti-Virus and software from McAfee and Associates. Both offer regular updates to handle newly discovered viruses.

Dangers of Downloading

The greatest risk to your privacy and to the security of your computer and data when web browsing is downloading files. Web browsers are downloading files even when it is not entirely obvious. Thus, the risk posed by downloading files may be present even if you do not actively go out and retrieve files overtly. Any file which you have downloaded from the Internet should be considered possibly dangerous (even files in the web browser's cache).

One thing to keep in mind is that if a computer is connected, any program has the capability of using the network, with or without informing you. Say, for example,

ANNEX F

Internet Security Tips
(Cont)

you download a game program from an anonymous FTP server. This appears to be a shoot-em-up game, but unbeknownst to you, it transfers all your files, one by one, over

the Internet to a hacker's machine! Because of these dangers, many corporate environments explicitly prohibit the downloading and running of software from the Internet.

Cookies Identify You

A cookie is a small file sent to your web browser by a web server to record your activities on a particular website. To block the cookie, set your browser to warn you before a cookie is written to your hard drive, or set it to reject all cookies. Here is how cookies work:

1. User clicks on a link
2. Web site sends info along with a "cookie" (a bit of data identifying that unique user).
3. Browser stores cookie on user's hard drive.
4. Next time user clicks on that site, cookie identifies user along with preferences and settings, etc.

Pitfalls of E-mail

All the normal concerns apply to messages received via Email that you could receive any other way. For example, the sender may not be who he or she claims to be. If Email security software is not used, it is very difficult to determine for sure who sent a message. This means that Email itself is a not a suitable way to conduct many types of business. It is very easy to forge an Email message to make it appear to have come from anyone. Another security issue you should consider when using Email is privacy. Email passes through the Internet from computer to computer. As the message moves between computers, and indeed as it sits in a user's mailbox waiting to be read, it is potentially visible to others. You should never send sensitive data via unprotected Email. Encryption programs are readily available, like PGP (which stands for "Pretty Good Privacy") for example, which offers a strong encryption capability.

One service many Email users like to use is Email forwarding. This should be used very cautiously. Imagine the following scenario:

A user has an account with a private Internet Service Provider and wishes to receive all her Email there. She sets it up so that her Email at work is forwarded to her private address. All the Email she would receive at work then moves across the Internet

ANNEX F

Internet Security Tips
(Cont)

until it reaches her private account. All along the way, the Email is vulnerable to being read. A sensitive Email message sent to her at work could be read by a network snoop at any of the many stops along the way the Email takes.

Most mail programs allow files to be included in Email messages. The files which come by Email are files like any other. Any way in which a file can find its way onto a computer is possibly dangerous. If the attached file is itself a program or an executable script, extreme caution should be applied before running it.

Modem Holes

You should be careful when attaching anything to your computer, and especially any equipment which allows data to flow. You should get permission before you connect anything to your computer in a centrally-administered computing environment.

Modems present a special security risk. Many networks are protected by a set of precautions designed to prevent a frontal assault from public networks. If your computer is attached to such a network, you must exercise care when also using a modem. It is quite possible to use the modem to connect to a remote network while still being connected to the "secure" net. Your computer can now act as a hole in your network's defenses. Unauthorized users may be able to get onto your organization's network through your computer!

Be sure you know what you are doing if you leave a modem on and set up your computer to allow remote computers to dial in. Be sure you use all available security features correctly. Many modems answer calls by default. You should turn auto-answer off unless you are prepared to have your computer respond to callers. Some 'remote access' software requires this. Be sure to turn on

all the security features of your 'remote access' software before allowing your computer to be accessed by phone.

Note that having an unlisted number will not protect you from someone breaking into your computer via a phone line. It is very easy to probe many phone lines to detect modems and then launch attacks.

Protect Your Password

An intruder may easily guess passwords unless precautions are taken. Your password should contain a mixture of numbers, upper and lower case letters, and punctuation.

ANNEX F

Internet Security Tips
(Cont)

Avoid all real words in any language, or combinations of words, license plate numbers, names and so on.

The best password is a made-up sequence (e.g., an acronym from a phrase you won't forget), such as "2B*Rnot2B" (but don't use this password!). Resist the temptation to write your password down. If you do, keep it with you until you remember it, then shred it! NEVER leave a password taped onto a terminal or written on a whiteboard. You wouldn't write your PIN code on your automated teller machine (ATM) card, would you? You should have different passwords for different accounts, but not so many passwords that you can't remember them. You should change your passwords periodically.

You should also NEVER save passwords in scripts or login procedures as these could be used by anyone who has access to your machine.

Be certain that you are really logging into your system. Just because a login prompt appears and asks you for your password does not mean you should enter it. Avoid unusual login prompts and immediately report them to your security point-of-contact. If you notice anything strange upon logging in, change your password.

Encrypt Everything

It is prudent to encrypt any file or e-mail message that is in any way sensitive. Be careful with the passwords or keys you use to encrypt files. Locking them away safely not only helps to keep them from prying eyes but it will help you keep them secure too; for if you lose them, you will lose your ability to decrypt your data as well! It may be wise to save more than one copy. This may even be required, if your employer has a key escrow policy, for example. This protects against the possibility that the only person knowing a pass phrase may leave the company or be struck by lightning. While encryption programs are readily available, it should be noted that the quality can vary widely. PGP (which stands for "Pretty Good Privacy) offers a strong encryption capability. Many common software applications include the capability to encrypt data. The encryption facilities in some of these programs are typically very weak.

Cleanup Your Browser

As you surf the Web, your browser both records the addresses of where you have been and stores downloaded files in a cache. If you want to keep this information from prying eyes, clear the temporary Internet files, delete the history files and the drop-down list under the address or location bar. While this may seem an extreme step, if you share a

ANNEX F

Internet Security Tips
(Cont)

computer, or use a public computer, consider doing this. If you use Explorer 5.0, under the Tools menu, select Internet Options. Now click on the General tab. Next, click on the Delete Files and Clear History buttons.

ANNEX G

Special Application Tools

1. When conducting any analysis with OSI, the need for automated support becomes almost immediately apparent. INSCOM analysts are able to draw upon a variety of different software tools during each phase of the analytical process using both classified and open source data. While the names, vendors, and functions of tools will constantly evolve, it is important for the analyst to understand what tools he currently should have access to, and what specific functions are these tools meant to perform that directly supports him. While the tools listed here are organized along the general lines of the OSINT analytical process, the analyst should note that the functions of each tool are not necessarily restricted to one particular process or analytical function. Also, while some tools are currently available throughout INSCOM, others are specifically resident within the INSCOM IOC or the IDC extensions.

a. This annex is not meant to provide a description of the overall INSCOM IOC architecture but of the tools that are used within INSCOM for OSINT analysis. It is important to note that virtually any data visualization and analysis tool can use OSI as readily as it can classified information. The format of the data is the important component of its compatibility with the tools, not its classification. The tools presented here are also not all inclusive of the tools available to the INSCOM analyst.

b. For information and task oriented training on the tools associated with the INSCOM IOC and IDC extensions, analysts should contact the INSCOM IOC Training Team for assistance. Training on tools are published 6 weeks in advance to allow analysts time to plan for attendance.

c. INSCOM's non-attributable Internet access policy or open-source search OPSEC procedures are classified.

2. Current OSINT related Tools within INSCOM

a. Collection Tools

(1) Internet Search Engines comprise the simplest and most user friendly method of conducting search of OSI for use of analysis. There are currently over 1500 different search engines available around the world. Search engines are used by more than 80% of Internet users with a combined total of 450 million searches conducted every single day. Using search engines is relatively easy for analysis since a majority of them only require Internet browser software like Microsoft Internet Explorer or Netscape Navigator. Listed below are some of the more general examples of search engines. While only a few search engines are listed here, a much more complete listing can be found at www.searchenginecolossus.com.

(a) www.google.com is a popular website that searches web pages not only according to your search terms, but also arranges the results according to the popularity of the site and number of links on other sites to the searched site.

(b) www.yahoo.com is currently the busiest search engine on the Internet. Like many other search engines yahoo has expanded to include newgroups, usergroups, peer to peer communications, and web-hosting among other services.

(c) www.vivisimo.com is a lesser known sight that uses a clustering engine, automatically organizes search or database query results into hierarchical folders. It is actually a meta-search engine that uses several other commercial search engines for its information.

(2) Lexis-Nexis is at www.nexis.com and offers a comprehensive collection of domestic and international news and business information sources from over 31,000 different sources. Results of queried information can be downloaded for integration with other data. Access to Lexis-Nexis information is through paid accounts.

(3) M3 (the Multimedia Message Manager, formerly known as AMHS), provides automated text message handling to the military, and civilian intelligence community in a system high environment. The M3 is the standard message handler for the Department of Defense Intelligence Information Systems (DoDIIS) community which provides: real-time dissemination of incoming message traffic based on user interest profiles; retrospective search of archive message database; and message composition, coordination, release, and validation. The M3 directly supports four (4) external communication links: Communications Support Processor (CSP), the AGT Gateguard, wire services (AP, UPI, Reuters), and Foreign Broadcast Information System (FBIS).

(4) COLISEUM stands for Community On-Line Intelligence System for End Users and Managers. It is a Defense Intelligence Agency (DIA) automated production/requirements management system. It provides the mechanism for registering and validating requirements, de-confliction of requirements, assigning and scheduling production, and provides the capability to track and manage overall production activities across operational and national planners and consumers. Like other applications listed in this document, COLISEUM was not designed to work exclusively with OSI, but supports the overall intelligence processes employed within INSCOM.

(5) Intelink/INSCOM Portal: Intelink is commonly perceived as simply the intranet/extranet that interconnects various intelligence organizations and operations. Intelink is actually a full suite of information services that have been put in place by various government organizations for their authorized users. It uses advanced technology such as commercial Internet applications and protocols, all operating on existing US Government as well as commercial telecommunications resources. Users can access open-source and classified intelligence products, exchange e-mail, access on-screen "video-on-demand," conduct video teleconferences, and use other tools that allow

users to collaborate or work together in real-time. The INSCOM Portal is the web-interface found on Intelink that allows registered users access to data, products, and web-based applications that are inherent to INSCOM and its IOC.

(6) MiTAP is a prototype system available for monitoring infectious disease outbreaks and other global events that is currently being adapted for specific INSCOM analytical requirements. MiTAP focuses on providing timely, global information access to medical experts and individuals involved in humanitarian assistance and relief work. Multiple information sources are automatically captured, filtered, summarized, and categorized by disease, region, information source, person, and organization. The articles are made available through a news server for remote access. Critical information is automatically extracted and tagged to facilitate browsing, searching, and sorting. A web-based search engine enables full text search of all documents stored in the archives. The system supports shared situational awareness through collaboration, allowing users to annotate existing documents, post directly to the system, and flag messages for others to see. MiTAP currently processes 3,000 to 15,000 articles daily, delivering up-to-date information to over hundreds of users.

b. Visualization and Analysis Tools

(1) Analyst Notebook (by i2 Solutions) is a link analysis / data visualization and sorting tool that enables the analyst to display large sets of data in a more comprehensive structure. Analyst Notebook is utilized within the INSCOM IOC organization to develop and track enemy network activity and organizations, Link / Trend Analysis, Center of Gravity (COG) charts, and information briefs. Analyst Notebook provides the capabilities for Analysts to:

(a) Create associate/network style charts

(b) Create sequence of events style charts

(c) Create and use attributes to aid in analysis

(d) Import external structured data to produce charts

(e) Use different representations to change the emphasis of a chart

(f) Use analytical tools to interrogate query and find data on charts

(g) Generate reports from the data held on in the charts

(h) Use presentation tools to explain convey details about a chart

(i) Exchange case studies between different units and agencies

(2) Pathfinder (by Pre-Search, Inc) is a Data Mining and Visualization application that is a powerful search application and tool set that allows you to locate the most pertinent information in large collections of data. The gateway to Pathfinder's tools is through a structured query language that enables the Memex text search engine to locate the desired information. However, as with most powerful applications, there are some skills to getting the most out of Pathfinder and the Memex search engine.

ANNEX H

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, overgeneralization 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.

ANNEX H

Categories of Misperception and Bias

(Cont)

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 selfabsorption 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.

ANNEX H

Categories of Misperception and Bias

(Cont)

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.

ANNEX I

Website 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 I edu / .gov I 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 web page's author is often embedded in the code.

   Who is the owner of the host server? Use WHOIS and DNS LOOKUP tools at http://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:web address) 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?

ANNEX I

Web Site Evaluation Checklist

(Cont)

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?**

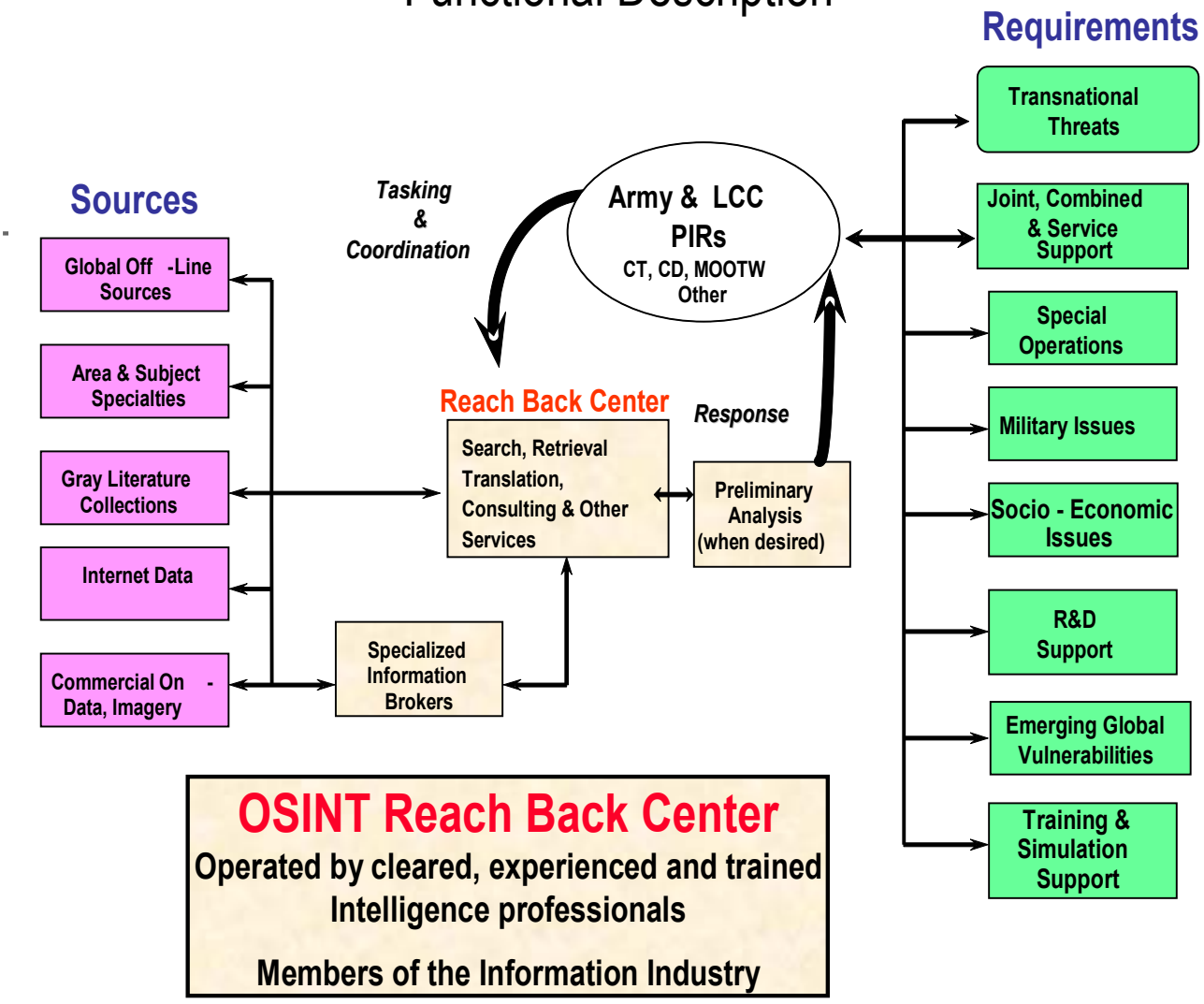
What's the page's aim, intent?
Why was it created?
Who sponsor's the page? Look for an "About us" entry.

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

ANNEX J

OSINT Reach Back Center

Functional Description



ANNEX K

References

a. Army Regulation (AR) 381-10, US Army Intelligence Activities (1 July 1984)

b. AR 381-11, Production Requirements and Threat Intelligence Support to the US Army (28 June 2000)

c. Department of Defense Office of General Counsel, Principles Governing the Collection of Internet Addresses by DoD Intelligence and Counterintelligence Components (6 February 2001)

d. Director of Central Intelligence Directive (DCID) 1/7, Intelligence Community Open Source Program (Draft, 3 April 2000)

e. Joint Pub 2-0, Joint Doctrine for Intelligence Support to Operations (5 May 1995)

f. Joint Pub 2-01, Joint Intelligence Support to Military Operations (20 May 1996)

g. Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence), DoD Cover and Cover Support Activities-Policy Clarification and Guidance (16 March 2001)

h. Office of the Assistant Secretary of Defense (Command, Control, Communications & Intelligence), Web Site Administration Policies & Procedures (25 November 1998)

i. Army Intelligence Master Plan (AIMP), Volume III, Enabling Architectures, Chapter 6, Open Source Information (OSI), (15 October 1996)

j. Aspin/Brown Commission Report: Preparing for the 21st Century, An Appraisal of US Intelligence (May 1996)

k. Open Source Exploitation: A Guide for Intelligence Analysts (Joint Military Intelligence Training Center, December 2000)

l. Open Source Intelligence Handbook (Joint Military Intelligence Training Center, October 1996)

m. NATO Open Source Intelligence Handbook, November 2001