

OSS ACADEMY

October 1998

**OPEN SOURCE
INTELLIGENCE:
EXECUTIVE OVERVIEW**

**Robert David Steele
Mark M. Lowenthal**

FORWARD

- 1. PURPOSE.** *Open Source Intelligence: Executive Overview* is published to ensure the dissemination of useful information that is vital to successful intelligence support to the policy maker, commander, and acquisition manager, but that may not yet be doctrinally available.
- 2. SCOPE.** This publication is based in part on two earlier publications, *Open Source Intelligence: HANDBOOK* and *Open Source Intelligence: READER*, the first of which was funded and published by the Joint Military Intelligence Training Center of the Defense Intelligence Agency. The material in this publication has been refined to provide a concise overview of open sources, software, and services pertinent to the collection and production of intelligence. Specific attention is given to the relationship between open source intelligence (OSINT) and all-source collection management, all-source analysis, coalition operations, and the creation of a “bare bones” OSINT Cell.
- 3. COPYRIGHT AND DISSEMINATION.** This document is an internal publication of OSS Inc. and is disseminated solely in connection with direct training. This document may not be reproduced without the explicit consent, in writing, of the copyright holders. Very modest fees are charged for electronic and hard-copy dissemination throughout organizations.
- 4. APPRECIATION.** This monograph would not have been possible without the earlier support of the Joint Military Intelligence Training Center (JMITC) of the Defense Intelligence Agency (DIA), and more recent support in the form of invitations to speak to the Australian conference on “Optimising Open Source Information” (Canberra, 7-8 October 1998), and to the Joint Intelligence Center (JIC) course at the Navy-Marine Corps Intelligence Training Center (Dam Neck, 19 October 1998).

Copyright © 1998 by OSS Inc.
Published by OSS Academy
4350 Fair Lakes Court, Fairfax, VA 22033 USA

All rights to text and illustrations reserved by OSS Inc. This work may not be copied, reproduced, or translated in whole or in part without written permission of the publisher, except for brief excerpts in connection with reviews, scholarly analysis, or professional briefings. Use with any form of information storage or retrieval, electronic adaptation or whatever, computer software, or by similar or dissimilar methods now known or developed in the future is also strictly forbidden without permission of the publisher.

ABOUT THE AUTHORS

Mr. Robert D. Steele, founder of OSS Inc. in 1992, serves as President and Chief Executive Officer of OSS Inc., President of OSS Global and also the Director of Collection for all OSS Groups. Mr. Steele has for seven years been the primary international focal point for open source intelligence training and advocacy. During this period he has organized seven international conferences and one European conference where over 4,000 international all-source professionals have been trained in various aspects of open source intelligence. He has consulted to eighteen governments, in each case training between 50 and 600 all-source intelligence professionals in open sources and methods. He is the primary author of the *Open Source Intelligence Handbook* (Joint Military Intelligence Training Center, October 1996), and lectures regularly at DIA and other U.S. military sites on open source intelligence as it applies to military all-source intelligence requirements. Mr. Steele has been twice named to the *Microtimes* 100 list of "industry leaders and unsung heroes who...helped create the future", and is featured in the chapter on "The Future of the Spy" in Alvin and Heidi Toffler's *WAR AND ANTI-WAR: Survival at the Dawn of the 21st Century*, among other publications. In the course of a twenty year national and defense intelligence career, Mr. Steele has fulfilled clandestine, covert action, and technical collection duties, been responsible for programming funds for overhead reconnaissance capabilities, managed an offensive counterintelligence program, initiated an advanced information technology project, and been the senior civilian responsible for founding a new national intelligence production facility. Mr. Steele holds graduate degrees in international relations (Lehigh University) as well as public administration (University of Oklahoma), and certificates in intelligence policy (Harvard University) and defense studies (Naval War College). He speaks fluent Spanish and elementary French, and holds a Top Secret clearance with current SBI.

Dr. Mark M. Lowenthal is Executive Vice President and Chief Operating Officer of OSS Inc., President of OSS USA and also the Director of Analysis and Production for all OSS Groups. He served as Staff Director of the House Permanent Select Committee on Intelligence (104th Congress, 1995-1997), where he directed the study *IC 21: The Intelligence Community in the 21st Century*. Dr. Lowenthal was a Deputy Assistant Secretary of State for Intelligence (1988-1989) and has also served as the Senior Specialist in U.S. Foreign Policy at the Congressional Research Service, Library of Congress (1989-1995). He is the author of seven books, including *U.S. Intelligence: Evolution and Anatomy*, which is a standard text in many intelligence courses, and over 80 articles and reports on national security issues. Dr. Lowenthal received his Ph.D. in History from Harvard University. He currently teaches graduate courses on intelligence at both Columbia University and George Washington University. In 1988, Dr. Lowenthal was the Grand Champion on *Jeopardy!*, the television quiz show. Dr. Lowenthal holds a Top Secret SI/TK clearance; OSS USA is fully equipped for support to SI/TK projects, to include STU-III voice and fax as well as secure storage.

4350 Fair Lakes Court, Fairfax, Virginia 22033 USA

Voice: (703) 242-1700 -- Facsimile: (703) 242-1711 -- Email: <oss@oss.net>

CONTENTS

1.0	INTRODUCTION	01
1.1	General Concepts	01
1.1.1	Presentation Plan	01
1.1.2	General Definitions	02
1.1.3	OSINT Timeline for Concepts and Doctrine	03
1.1.4	Open Sources and the Intelligence Community	04
1.1.5	Definition of Open Source Intelligence (OSINT)	04
1.1.6	What OSINT is <i>Not</i>	05
1.1.7	OSINT and the All-Source Process	07
1.1.8	The New Intelligence Gap	09
1.2	The Larger Context	10
1.2.1	The Larger Context for OSINT Exploitation	10
1.2.2	Intelligence Community Leadership Perspectives	15
1.2.3	Costs and Purposes of Secrecy	16
1.2.4	OSINT Valuation Metrics	18
1.2.5	The Reality of OSINT	19
1.2.6	The Burundi Exercise	21
2.0	OPEN SOURCE INTELLIGENCE OVERVIEW	22
2.1	Open Sources	22
2.1.1	The Open Source Marketplace	22
2.1.2	Current Awareness Basics	23
2.1.3	Geospatial Shortfalls and OSINT Solutions	24
2.2	Open Software	29
2.2.1	Software Functionalities	29
2.2.2	Data Visualization	30
2.2.3	Data Exploitation	31
2.3	Open Services	32
2.3.1	Data-Oriented Services	32
2.3.2	Human-Oriented Services	33
2.3.3	Information Brokers	34
2.3.4	Geospatial Visualization	35
2.3.5	Citation Analysis	38
2.4	OSINT Overview	39
2.4.1	OSINT Issue Areas	39
2.4.2	OSINT Rules of the Game	40
2.4.3	The Reality of the Internet	41
2.4.4	OSINT as a <i>Process</i>	43
2.4.5	Integrated OSINT Concept	44

3.0	OSINT AND COLLECTION MANAGEMENT	45
3.1	General Uses of OSINT	45
3.2	OSINT as a Foundation	46
3.3	The Changing Collection Paradigm	47
4.0	OSINT AND ALL-SOURCE ANALYSIS	48
4.1	The Changing Analysis Paradigm	48
4.2	Changing Role of the All-Source Analyst	48
4.3	OSINT and Multi-Level Analysis	49
4.3.1	OSINT and Threat Analysis	50
4.3.2	OSINT and Strategic Generalizations	51
5.0	OSINT AND COALITION OPERATIONS	52
5.1	Intelligence Upside Down	52
5.2	OSINT Contributions to Coalition Operations	53
5.3	Creating a Joint OSINT Cell and Network	54
5.4	OSINT Contribution to Own Force Coordination	55
6.0	CREATING A “BARE-BONES” OSINT CELL	56
6.1	General Purpose	56
6.2	Specific Functionalities	56
6.3	Typical Products	57
6.4	Staffing Concept	58
6.5	Recommended Approach	59
6.6	Persistent Problems	60
6.7	Budgetary Recommendations	61
7.0	CONCLUSION	63
7.1	Military Leadership	63
7.2	Information Operations Big Picture	63
7.3	Virtual Global Intelligence Community	64
7.4	Intelligence Reform: Striking a New Balance	65
7.5	Revolution in National Security Affairs	67
7.6	National Information Strategy	68
7.7	OSINT Building Blocks	69
7.8	Information-Driven Government Operations	70
8.0	NOTES	71
8.1	References	71
8.2	Training	72
8.3	Endnotes	73

1.0 INTRODUCTION

A full appreciation of the emerging discipline of open source intelligence (OSINT) requires both an understanding of several general concepts as well as the larger context within which OSINT is made possible.

1.1 General Concepts. Among the general concepts that are important to understanding how OSINT fits into the all-source intelligence collection and production model are those dealing with the distinctions between data, information and intelligence; and with the nature of the environment

1.1.1 Presentation Plan. Here is the plan for the presentation. The heart of the matter is the nature of the open source world, and that is where we will spend much of our time.

I n t r o	Overview of Open Sources, Software and Services	C M	A n a l y s i s	C o a l i t i o n s	e l l	o n c l
-----------------------	---	--------	--------------------------------------	--	-------------	------------------

Figure 1: Presentation Plan

It is, however, important that open sources be understood in context, and in relation to larger issues including intelligence reform, national information strategies, and information operations, so we will have substantive introductory and concluding remarks.

Finally, no concept should be presented without some specifics as to applicability, so we will have four slices, one each on open sources in relation to collection management, all-source analysis, and coalition operations, and a fourth slice on creating a “bare bones” OSINT Cell and what one might budget for national or defense OSINT operations.

This handout contains all of the information and all of the illustrations used in the Open Source Intelligence Operations Course.

A number of core references for further study, almost all of them available at no cost on the Internet, are identified at the end of this paper, together with several training opportunities.

1.1.2 General Definitions. We speak of business intelligence, or national intelligence, or military intelligence, as if intelligence were a generic organizational capability, and in some ways it is. However, we need to get back to basics if we are to improve our understanding of the world.

DATA: raw report, image or broadcast.

INFORMATION: collated data of generic interest and usually widely disseminated.

INTELLIGENCE: concisely tailored answer reflecting a deliberate process of discovery, discrimination, distillation and delivery of data or information that has been evaluated, collated, filtered, and presented to meet a precise need, generally from a single decision-maker.

Figure 2: Definitions

- DATA is what you would expect.
- INFORMATION is generic collations of data, generally broadcast to large numbers of individuals.
- INTELLIGENCE is a process that answers questions *for specific individuals*.

Using these definitions, one would surmise that 90 to 95% of any national or military intelligence organization's production is actually classified *information* rather than classified *intelligence*.

At the same time, it merits comment that nowhere is it written that "intelligence" is by definition classified. It is possible to create very useful intelligence using only open sources, and to produce intelligence without secrecy, and this is where national, military, law enforcement, and business community interests intersect.

1.1.3 OSINT Timeline for Concepts and Doctrine

2004	Soonest possible date by which genuine integration anticipated
1992	OSINT Revolution Begins OSS Inc. created, first OSINT conference DCI's Open Source Coordinator appointed Society of Competitive Intelligence Professionals (SCIP) begins to grow
1947-1992	Special Librarians Association joins up to 16,000 members External research & analysis funds create contractor community Lloyd's of London, and Jane's Information Group, set new standards BBC and then FBIS create broader networks
1941-1947	Office of Strategic Services (OSS) created Central Intelligence Group and then Agency followed
* 1930's	Winston Churchill used personal networks and correspondence wisely
300 B.C. on	"Legal travelers" and word of mouth were the standard source

Figure 3: Timelines for Concepts and Doctrine

Open Source *Information* is not new. Long before the Roman Empire we had legal travelers and scholars. Even Open Source *Intelligence* is not new in that we have long appreciated the intelligence value of open sources. What *is* new are three things:

First, we lost our way. The Office of Strategic Services, the original OSS, and its follow-on the Central Intelligence Group and then the Central Intelligence Agency, were created primarily to coordinate disparate sources of information and to do strategic *analysis* using predominantly *open* sources. Ultimately we ended up relying very heavily on classified technical collection and secret human sources....but that is another story.

Second, we are now starting to understand the limitations of secret sources and methods—not to mention their cost—at the same time that we are coming full circle in a globalized economy with no environmental or ideological boundaries, and beginning to see the extraordinary value to citizens, governments, and to intelligence communities, of an open source foundation. Since 1992 at least eighteen governments have taken serious but not necessarily effective looks at what open source intelligence might contribute to their all-source endeavors.

Third, and we have alluded to this, some of us are starting to envision truly *national* intelligence communities, as well as a global “virtual intelligence community”, in which open information sharing and open source intelligence production is commonplace. We have decades of hard work ahead.

1.1.4 Open Sources and the Intelligence Community

“The Intelligence Community has to get used to the fact that it no longer controls most of the information.”

The Honorable Richard Kerr
Deputy Director of Central Intelligence (USA)

Figure 4: Open Sources and the Intelligence Community

The business community faces a situation analogous to that of the Intelligence Community in that it can no longer “muddle through,” relying only on its legacy data and the seat of the pants knowledge of its managers and its engineers and its sales force.

Peter Drucker, writing in *FORBES ASAP* on the 24th of August 1998, restated a thesis he has been pursuing for around three years now: focusing on internal *data* and information *technology* is not a path to prosperity.

Drucker focuses our attention instead on the next revolution in both business and intelligence, the development of an effective *information* system (not necessarily involving technology) for top management that provides for the collection and organization of *outside* information.

The open source intelligence revolution, which several of us started in 1992, takes this one step further, both for the intelligence communities of the world, accustomed to dealing with internal secrets, and for the business communities of the world, accustomed to muddling through without “intelligence” as we know it.

1.1.5 Definition of Open Source Intelligence (OSINT)

Open Source Intelligence (OSINT) results from the integration of legally and ethically available multi-lingual and

multi-media sources, with the heretofore largely secret processes of national intelligence: requirements analysis, collection management, source validation, multi-source fusion, and compelling presentation.

<p>From the Open World</p> <ul style="list-style-type: none"> - Open sources - Open software - Open services 	<p>From the Closed World</p> <ul style="list-style-type: none"> - Requirements analysis - Collection management - Source validation - Source fusion - Compelling presentation
--	---

Figure 5: Elements of OSINT

We approach Open Source Intelligence with three premises in mind:

First, that the private sector now controls roughly 90% of the pertinent information for creating both open and secret intelligence;

Second, that within the private sector are niche experts on any given topic or any given source whose expertise cannot be matched within any given intelligence community; and

Third, that the private sector really does not know very much about the proven *process* of intelligence that has heretofore been largely secret by inclination rather than necessity.

Hence, what is new about Open Source Intelligence is that it seeks to integrate the wealth of sources, software and services from the private sector, with the proven and heretofore largely secret process of intelligence.

1.1.6 What OSINT is Not

As we will find as we go through this brief, OSINT requires both the full exploitation of all available sources, and also the application of the proven methods of intelligence. One effective means of framing the discussion is to address very early on what OSINT is *not*.

- OSINT is *not* a collection of news clippings.

- OSINT is *not* the Internet.
- OSINT is also *not* a substitute for spies or satellites or other sensitive collection capabilities.

“...nothing more than a collection of news clippings”.

“...the Internet”

“...a substitute for spies and satellites.”

Figure 6: What OSINT is *Not*

OSINT is not a substitute for spies or satellites or other sensitive collection capabilities. Evil and conflict are a natural condition of man. As our national infrastructures and social fabric become increasingly complex and vulnerable to attack by individuals and gangs, it will be ever more imperative that our clandestine collection capabilities be fully effective. OSINT is the foundation for both all-source collection and all-source analysis, and not to be confused with their result.

In fact, we distinguish between OSINT, which can be produced in the private sector by organizations such as ours, and Validated OSINT, or OSINT-V.¹

Validated OSINT can only be produced by all-source analysts who have access to the complete range of classified sources and all-source analyses, and who are able to state with certainty that the OSINT they are validating is either consistent with classified understandings, or that there exist no classified findings in contradiction to the validated OSINT.

OSINT is the foundation for both all-source collection and all-source analysis, and must not be confused with their all-source result.

In the business world, one could say that OSINT should not be confused with the intuitive judgement of the executive, for whom OSINT is a valuable resource, but no substitute for the *gestalt* of management.

1.1.7 OSINT and the All-Source Process

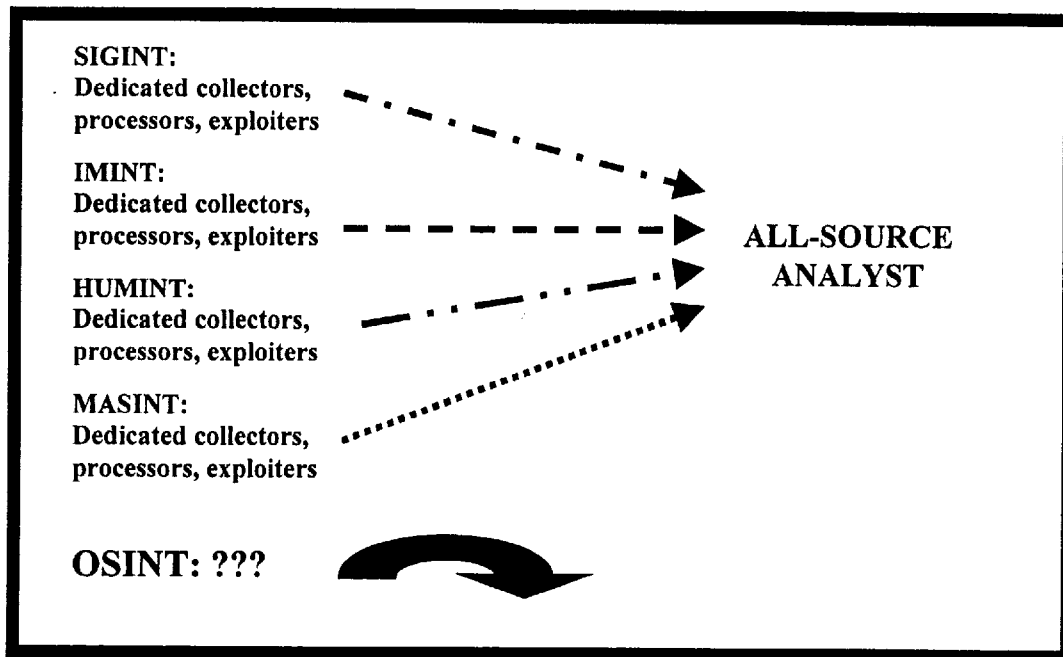


Figure 7: The Missing Element of the All-Source Process

We spend billions each year on the three traditional and one relatively new classified disciplines, and each of these disciplines has dedicated collectors, processors, and exploiters. OSINT has no similar organizational, financial, or expert infrastructure.

Although libraries exist, we need to emphasize again and again that OSINT is vastly more complex in terms of sources, human expert coordination, commercial imagery exploitation, and general financial and legal demands, than any normal library can cope with.

OSINT requires the same level of commitment that each of the traditional disciplines receives, and in fact—as the “source of first resort”—might reasonably call for the assignment of the best and the brightest collection and analysis

personnel, in that their successes with open sources will dramatically improve and extend the contributions of the traditional disciplines.

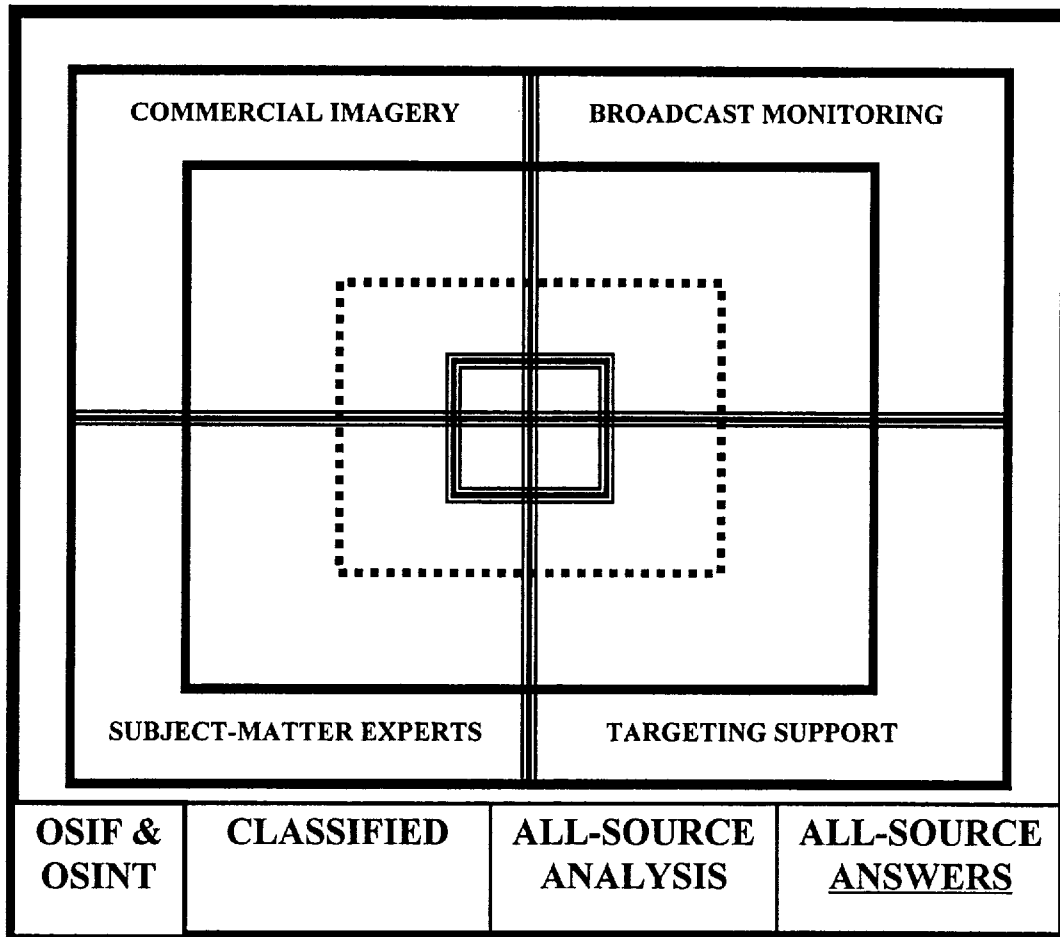


Figure 8: OSINT Fully Integrated into All-Source Collection and Analysis

OSINT can be treated as a separate discipline, but once fully matured, would be best if it were given a split-personality: at once fully integrated into the routine operations of the four traditional disciplines, but also handled as a separate discipline in order to ensure that imagery, to take one example, receives the full benefits of broadcast tip-offs and human subject-matter experts on forthcoming events.

The recent Indian-Pakistani nuclear bake-off provides a good case study of how a much wider OSINT net might have readily found the print announcements of forthcoming testing; the scholarly analysis in February, in English, of the

significance of the political parties commitment to nuclear testing, the benefits of alternative imagery platforms (Russian, commercial) in monitoring the testing areas, and so on.

It merits comment, in this context, that most of our so-called secret methods really are not secret at all. The Indian government knew to the minute when our classified satellites would be passing over and what their angle of look is. Most governments world-wide know who our clandestine personnel are and who most of our agents are. We need to think of the all-source solution as one that will reduce expense, increase effectiveness, and in passing permit a makeover of our classified capabilities so they can return to the secret world.

1.1.8 The New Intelligence Gap

We conclude our introductory discussion of general concepts with a look at the new intelligence gap.²

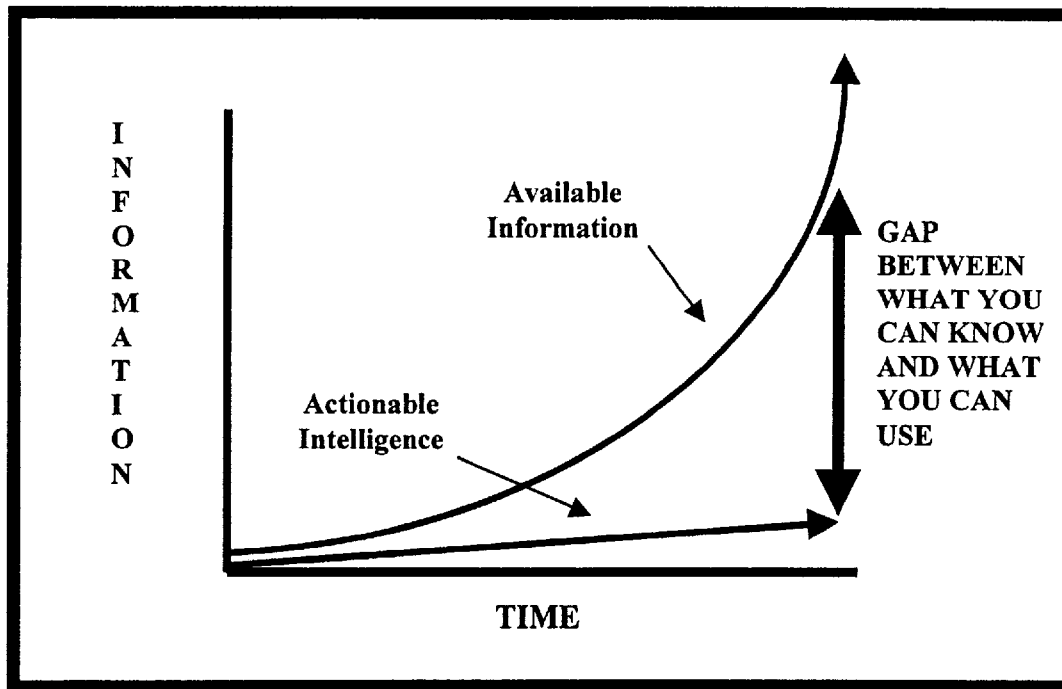


Figure 9: The New Intelligence Gap

At first glance, it would seem that the age of the information revolution would be the *best* time for decision-makers to get the information they need. The reality is quite the opposite for four major reasons:

- Too Much Information
- Too Many Potential Sources
- Increasing Aversion to Technology
- And No End in Sight

Faced with these apparently insurmountable problems, decision-makers and, indeed, offices within their organizations responsible for providing information and intelligence most often make one of two harmful choices:

1. they either avoid the issue entirely and rely on their own limited reading time to get the information they think they need; or
2. they create wholly inadequate products, such as clipping collections or news summaries.

The result: a new intelligence gap.

1.2 The Larger Context. The all-source intelligence process does not take place in a vacuum. The most significant change in the intelligence process is that classified sources are no longer sufficient, and the intelligence community simply cannot control most of the information of import to its consumers.

1.2.1 The Larger Context for OSINT Exploitation. Below we examine three aspects of the larger context for OSINT exploitation in the all-source intelligence process: the larger information environment within which intelligence operations take place; the changing nature of the threat; and the demands of multi-level analysis heretofore ignored by intelligence professionals.

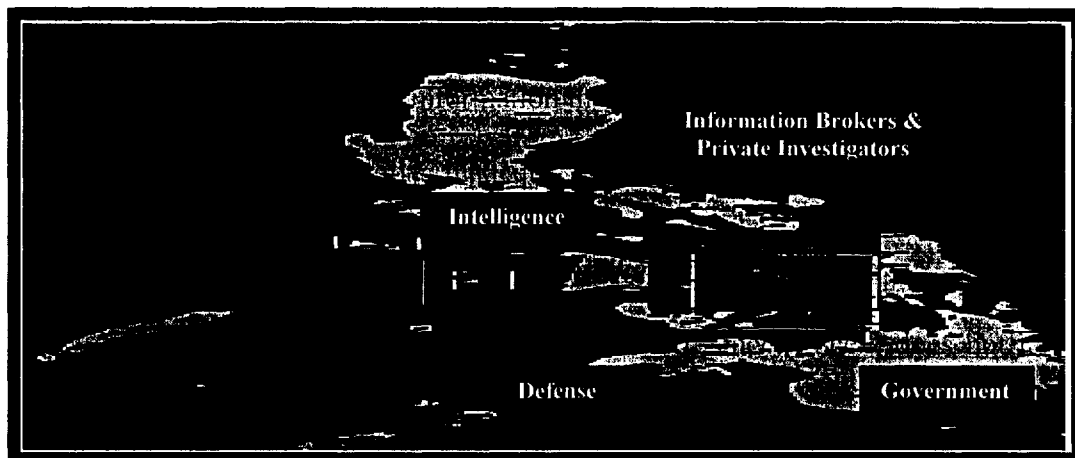


Figure 10: The Larger Information Context for Intelligence Operations

The private sector contains many communities, each with their own unique access to open sources, software and services. Unfortunately, this vast range of offerings comes in the form of an archipelago rather than a smooth menu. Now to mix metaphors.....

- There are *iron curtains* between the communities.
- There are *bamboo curtains* between the organizations within each community.
- There are *plastic curtains* between the individuals within each organization.

Navigating this archipelago, and being able to drill down to discover the right mix of sources, bring them together within the right mix of software, and assure the client that one is also exploiting the right mix of services, is no easy task. It merits comment that the intelligence community is a relatively small island among these other much larger islands.

There is another aspect to this larger context for intelligence community operations, and that is the ever-growing complexity of the threat.

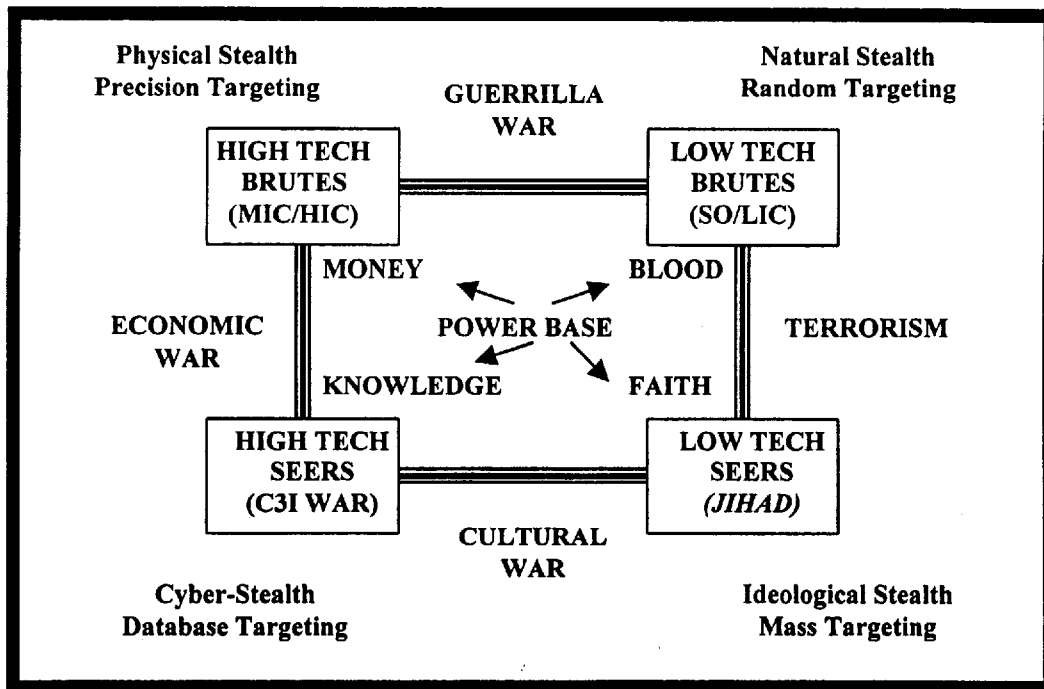


Figure 11: Complex Threat Amenable to Open Source Intelligence

This figure and the next are important because they emphasize the increased value of open source intelligence.

Our defense and intelligence communities are optimized for attempting to monitor and understand only one of these four warrior classes, the high-tech brute.

Fortunately, each of the other three warrior classes can be largely monitored and relatively well understood through the use of open source intelligence—but we do not have the funding in place, the concepts or doctrine, and the organizational mechanisms to assure our governments and our corporations of the proper application of open source intelligence to these challenges.

This is not to say that we do not need spies and satellites and such. On the contrary, each of the four warrior classes will continue to require special sources and methods to be used in the pursuit of that information that cannot be acquired through open source intelligence. Indeed, that narrow range of extremely sensitive information will become much harder to acquire as the world becomes more complex, hence there is no basis for suggesting that the increased value of open sources should lead to a reduction of funding for classified sources.

A-/B+	OBVIOUS MILITARY WE DO WELL ENOUGH	CRIME AND TERROR WE DO BADLY	C-/D+
	REGARDING CYBER-WAR WE ARE "SICK IN QUARTERS"	IDEOLOGY AND ENVIRONMENT WE DON'T DO AT ALL	
SIQ			D-/F+

Figure 12: The Good, The Bad, and The Ugly Truth about Intelligence³

The juxtaposition of these newly complex threats—those that would do us harm—interlaced with the every-increasing vulnerability of our electronically-based critical infrastructures, the globalization of the economy, and the empowerment of previously fragmented groups through information technology, not only increase the value of open source intelligence, but also raise the bar so high for national intelligence that the traditionally classified intelligence community has no alternative but to embrace OSINT while also refocusing its precious classified capabilities as narrowly as possible so as to succeed against increasingly “mission impossible” types of targets.

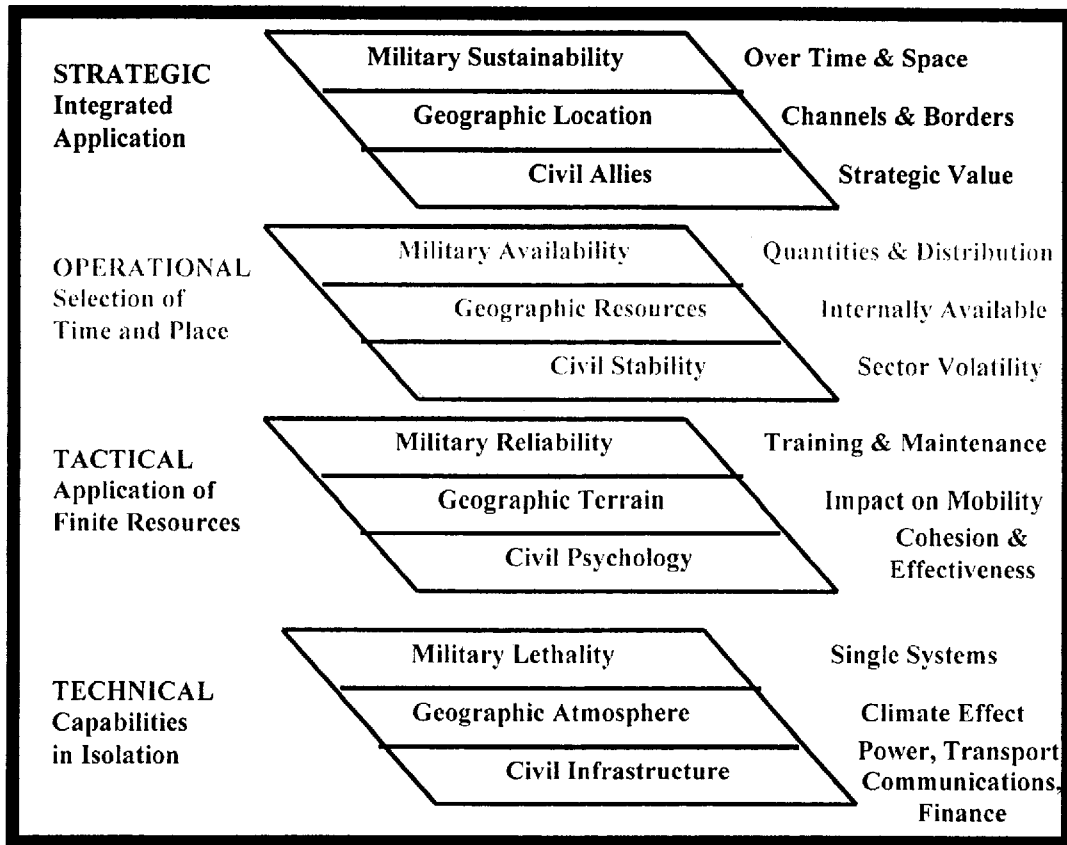


Figure 13: OSINT as a Major Factor in Supporting Multi-level Analysis

This figure is important because it represents both the levels of analysis at which intelligence should be created, and also the integrative aspects of intelligence, where military capabilities cannot and should not be evaluated without regard to the geographic conditions and civil factors.

Open source intelligence can satisfy 80% of the requirements over these four levels of analysis.

This figure will appear again. For now, contemplate the reality that we only do technical or worst case threat analysis, and we look at military, geographic, and civil factors in isolation from one another. More on this later. For now, only the grades.

Intelligence is not making a sufficiently significant contribution to deciding what we build, when we fight, or what we use.

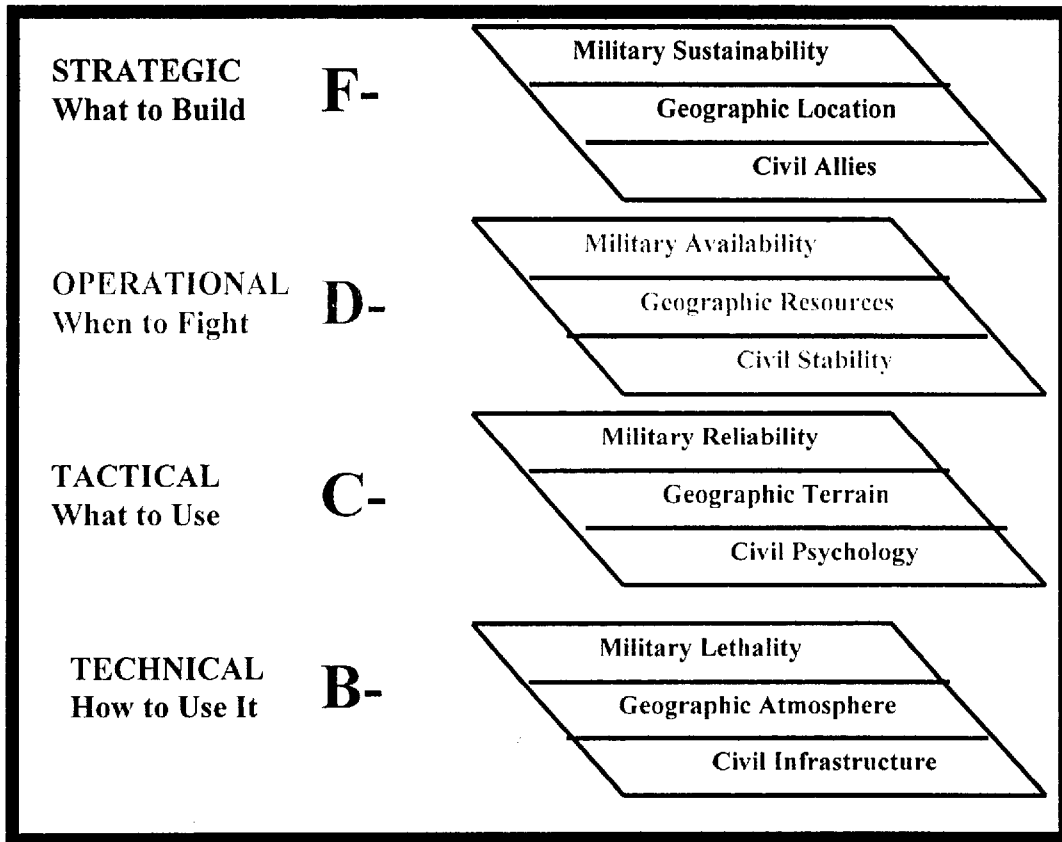


Figure 14: Intelligence Failures at Each Level of Analysis

We do well enough with how we use specific capabilities, but one has to wonder if \$79 million dollars worth of precision munitions, half of which did not hit the intended targets, was an effective means of killing roughly 26 people and

wounding another 40 during the recent strikes into Afghanistan.⁴ While this was a policy decision, and one can speculate that the goal was to make a point rather than kill or wound a specific number of people, the issue remains: was national and defense intelligence able to offer the policy-makers a sufficiency of alternative courses of action and the underlying operational intelligence necessary to provide genuine choice?

1.2.2 Intelligence Community Leadership Perspectives

Now for some mixed news. Our very best intelligence leaders have always understood, and still understand today, the value of open sources of information. Most of them still do not understand the difference between open source information and open source intelligence, but that should not be surprising since they also don't understand the difference between classified information and classified intelligence.

From the 1940's to date, the generally accepted percentage of intelligence requirements that open sources are able to satisfy is 80%. In the United States, open sources—and poorly accessed open sources at that—are officially credited with contributing 40% of the final all-source production content, at a cost of 1% of the total cost of national intelligence across the board.

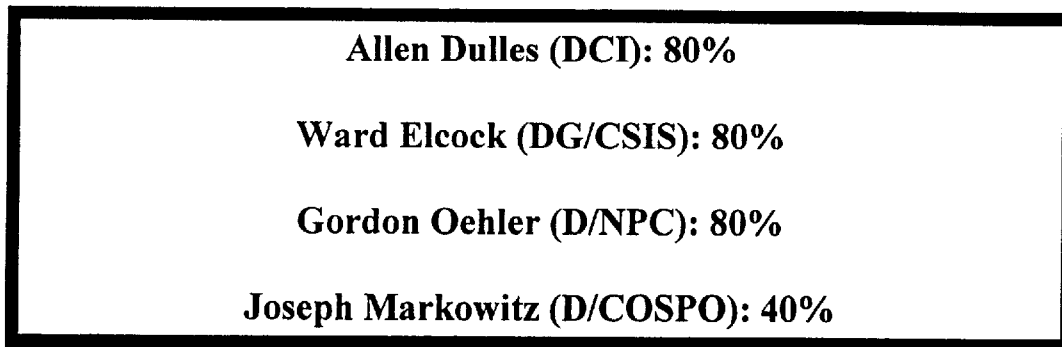


Figure 15: Authoritative Estimates Regarding Open Source Contribution⁵

The lower estimate of Dr. Markowitz is especially interesting because it was based on rigorous study within the Central Intelligence Agency that also documented the fact, publicly stated, that this result was achieved at a cost of just 1% of the total National Foreign Intelligence Program (NFIP) budget.

Generally, most professionals fully familiar with both open source capabilities and all-source requirements will agree that the contribution of open sources can be as little as zero (or 10% in peripheral targeting support) or as much as 95%, as suggested by the Commission on Intelligence with respect to strategic economic intelligence products.⁶

In the U.S., we spend \$250 million per year for open sources, and roughly \$25 billion per year for classified sources. This dichotomy should give us pause.

Again, this is not to suggest that we should reduce our spending on spies, satellites, and such, only that we must take care to avoid conducting our espionage in such isolation from open sources as to fail in a ridiculous manner.

1.2.3 Costs and Purposes of Secrecy

Professional intelligence officers have an obligation to think about more than simply getting an accurate, complete, sensational intelligence report out the door. Our secret sources and methods exact a great cost, certainly greater than most understand, and very likely greater than any of us would be willing to pay if we did understand.⁷

Clients are deluged with information, much of it purporting to be intelligence. They simply do not have the time to read through compendiums of classified information in order to extract, themselves, the nuggets of intelligence that may be contained therein.

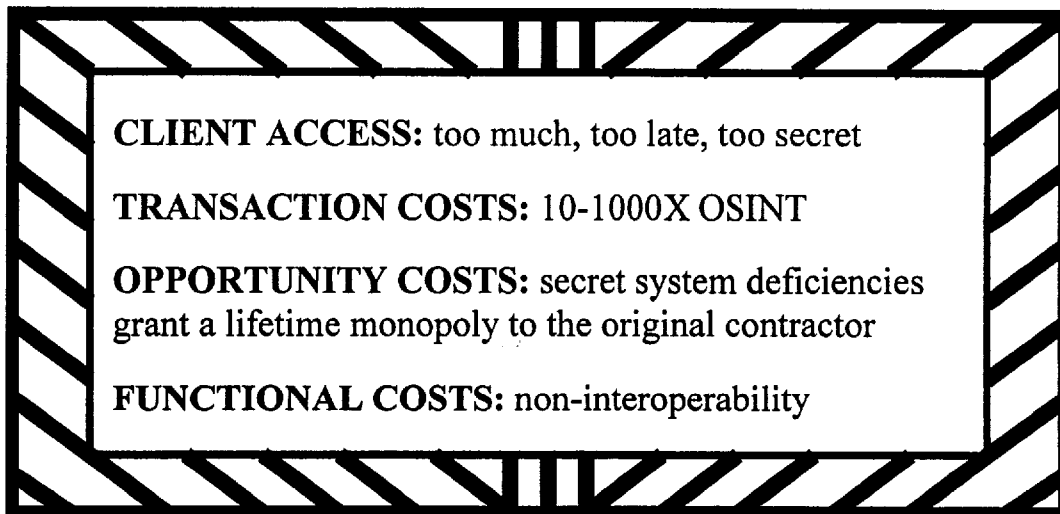


Figure 16: The Not-So-Hidden Costs of Secrecy

We cannot afford the extraordinary expense of secret sources and methods when ordinary open sources and methods will do. We must conserve our precious classified capabilities for those extraordinary needs.

In Figure 19 we will see a commander's statement on the relative merits of too many secrets, late, versus open source intelligence in time, but for now, let us focus on the fact that our most important determinant of success is access to our clients and constructive contributions to their decisions. If excessive secrecy prevents them from reading or digesting our classified information, then it is we who must change our methods, not they who must change their habits.

In a down-sizing government, as financial crises buffet Asia on the one side and Russia on the other, we must be very conscious of costs. Intelligence is no longer immune from fiscal accountability, and secrecy should not be used to conceal ineffectiveness.

Classifying deficiencies prevents the smart people in California, most of whom would never pass a security check, from offering Sunnyvale-like solutions.

Compartmented systems are inherently not interoperable with one another, or with the operational systems they are intended to support.

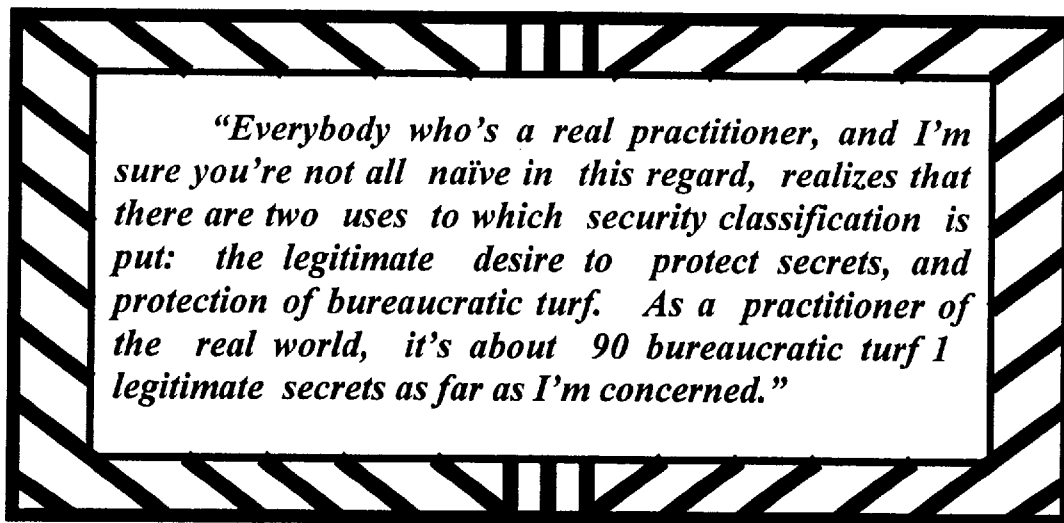


Figure 17: The Truth and Nothing But the Truth

Rodney B. McDaniel, then Executive Secretary of the National Security Council and previously the Senior Director of the Crisis Management Center in the

Executive Office of the President, said the following to a group of very senior policy-makers and intelligence professionals meeting at Harvard University.⁸

This sums it up. 90% of the secrecy that we consider so precious is in fact not necessary.⁹

At the same time, we must not conclude that there is no need for secrecy!

CAVEAT: This is not to say that we do not need secrets, nor is it to say that some intelligence, such as ULTRA in World War II, does not merit extreme secrecy and the costs attendant to that secrecy. Our focus is on the general good, not the specific exceptions that fully warrant extreme attention to the traditional principles of espionage.

Figure 18: Caveat on Relative Value and Cost of Secrecy

1.2.4 OSINT Valuation Metrics. As we evaluate open sources, whether against classified sources or for the inherent value of our investment in open sources as opposed to not investing at all, we have to ask ourselves:

- **TIMING:** Do open source enable good enough information to be received *quickly*?
- **CONTEXT:** Do open sources give us a *contextual understanding* that would not otherwise be available?
- **CONTENT:** Are open sources “good enough” to *improve the decision at hand*, whether by reducing uncertainty or bringing forward factors that would otherwise have been overlooked?
- **EMPOWERMENT:** Perhaps even more valuable: does the inherent sharability of open sources empower the decision-maker by contributing to the understanding of other key personnel, most of whom may not be cleared for proprietary or classified information?

Experience has shown that there are two valuable external considerations associated with open source information or intelligence:

- RETURN ON EXPOSURE: Does this information, openly available, attract other information that is equally useful?
- INCLUSIVENESS: Does this information, openly available, reach those who have a “need to know” that would not otherwise have been included in distribution?

First, open information tends to attract other open information that is useful and would not otherwise have been received. The Lake Tahoe Hackers Group, discussing the inherent value of sharing on the Internet, concluded that for every item they posted on the Net, they tended to receive 100 items back, directed to them, of which ten were new and useful. Our experience through our web site, www.oss.net is consistent with this. A 10 to 1 return on investment--not bad!

Second, information openly available has a tendency to be found by people who have a genuine need to know but who would not have been reached through pre-planned distribution, whether classified or not. At least ten percent, and more likely twenty percent, of the people you really need to reach are not reachable through existing bureaucratic practices.

1.2.5 The Reality of OSINT

Analysts continue to forget that the operational world has a timetable. Perfect, complete, well-balanced reports that are late are useless. The same is true of reports that require TIME to digest.

“If it is 85% accurate, on time, and I can share it, this is a lot more useful to me than a compendium of Top Secret Codeword material that is too much, too late, and needs a safe and three security officers to move it around the battlefield.”

**U.S. Navy Wing Commander
Leader of First Flight Over Baghdad
Speaking at TIG-92, Naval War College**

Figure 19: Operational Realities Affecting OSINT's Value

Commanders and staff need to learn that they have the right to not only define the intelligence requirement, but to instruct the intelligence professional as to how long the answer will be, how long the intelligence community has to answer the question—be it minutes or hours or days—and—understand this clearly—HOW LONG THE ANSWER MAY BE—whether a yes or no, a paragraph, or a page.

Intelligence professionals must be ready to accept such guidance and perform accordingly.¹⁰

Post-Cold War political-military issues tend to arise in lower Tier (per PDD-35) nations where U.S. classified capabilities are least applicable or largely unavailable.

Warning of these largely Third World crises has not required classified collection or analysis.

Policy approaches and transnational resolution have required increased reliance on international organizations and non-traditional coalition partners with whom information must be shared and who are not “cleared” for sensitive sources & methods.

Figure 20: Global Realities Affecting OSINT's Value

The Director of Central Intelligence (DCI) has acknowledged publicly that he cannot do global coverage with the resources he has, as they are consumed by the hard task of monitoring the higher tier priorities. He also understands, as do most senior leaders (but not their middle managers), that open sources offer an ideal means of dealing with the requirements of global coverage, at very low cost.

Most of our political-military issues are in countries that are lower tier until they emerge as crises, and thus they are not well covered by classified capabilities up to that point—nor can classified resources be readily diverted or applied on short notice. Most crises in the Third World are clearly identified by open source reporting. Both war-fighting and peacekeeping in the Third World now require the active involvement of the United Nations, various non-governmental organizations, civilian agencies, and coalition partners not even remotely familiar with—nor cleared for—the horrible Top Secret architecture through which both NATO and the US/UK/CAN/ANZ coalitions operate.

Reality demands that we develop a robust international OSINT network.

1.2.6 The Burundi Exercise

There has actually been a formal benchmarking exercise conducted. It was done at the direction of the Commission on Intelligence (USA), and began at 1700 on Thursday 3 August 1995. Open source collection was completed by close of business the next day, and the results received by the Commission at the appointed time, via overnight mail to their offices, arriving at 1000 on the Monday.



UN/US OPS, POL-MIL SUMMARY	Twenty-Two POL-MIL Overviews Oxford Analytica (Oxford, UK)
SOURCES ON THE GROUND, BIOGRAPHICS	Top Ten Journalists in the World LEXIS-NEXIS (Miamisburg, OH)
CULTURAL AND TRIBAL HISTORIES	Top Ten Academics in the World Institute of Scientific Information (Phil., PA)
DETAILED OOB AND PRECIS'S OF TWO YEARS REPORTING	<i>Tribal</i> Orders of Battle/Areas of Influence Janes Information Group, Coulsdon, UK
	1:100,000 "Soviet" Military Combat Figures East View Publications (Minneapolis, MN)
	1:50,000 Imagery, Cloud-Free, <3 Years Old SPOT Image (Toulouse, FRANCE)

Figure 21: The Burundi Exercise: "John Henry" Beats the Steam Hammer

This was a classic exercise in which one person's *Rolodex* ("knowing who knows") was able to bring to bear the full force of the private sector's considerable capabilities through just five telephone calls.

The U.S. Intelligence Community, for whom Burundi was neither a higher-tier monitoring requirement nor—even in crisis—a sufficiently high priority for surge collection, had essentially nothing to compare with the open source information that was presented to the Commission on Intelligence "overnight".

What was delivered from the international private sector was not open source intelligence *per se*, as no integrated analysis was provided and specific operational questions were not answered, but these could easily have been provided over the week-end had this been part of the task.

For both early surge support and on-going global coverage, open sources of information represent the only viable solution.

2.0 OPEN SOURCE INTELLIGENCE OVERVIEW

2.1 **Open Sources.** In this first of three sections we will introduce the open source marketplace™ and focus on specific examples of sources useful to the all-source intelligence professional (both collectors and producers).

2.1.1 **The Open Source Marketplace™.** We have already discussed what OSINT is *not*. It is *not* merely a collection of news clippings, and it is *not* the Internet. Nor is it the aggregation of all of the sources, software and services selectively listed here.¹¹

- a. **SOURCES:** Include current awareness, academic journal, and archival sources; directories of experts and conferences; a wide variety of both online and offline sources with various types of value-added including indexing, translation, and abstracting; and many multi-media forms of data including maps, charts, and commercial imagery.
- b. **SOFTWARE:** Encompasses a full range of commercial off-the-shelf offerings that provide Internet access, data entry and retrieval tools, automated translation and abstracting, data mining and visualization, desktop publishing and collaborative communication tools, and electronic security tools.

- c. SERVICES: This least understood and most valuable aspect of the open source world spans a full range of specialty support services, from subject-matter and language-qualified experts in online retrieval to experts in gray literature discovery; from media to directed primary collection including telephone surveys, private investigations and legal traveler reconnaissance; and more complex market research and strategic forecasting services.

The above sub-paragraphs are intended to suggest—but not comprehensively list—the enormous range of sources, software and services available within the private sector.

OSINT is created when one properly defines the requirement, brings together the right sources, applies the right software, takes advantage of the right services, all in order to produce an answer to a question of specific interest to a specific client.

Most intelligence communities, and most businesses, have a very limited understanding of the full range of options in the private sector; they have no means for judging “best practices” between private sector options; and they generally do not have a procurement or cultural environment that will permit them to “mix and match” what they need from this complex world.

2.1.2 Current Awareness Basics. Here are some representative “bits” that one must combine in order to have a moderately successful program for monitoring any given topic of interest.

- Dow Jones Interactive, although new to the marketplace, has already emerged as a front runner, combining web-based access and an easy to use interface, with an impressive array of sources. It is our first choice.
- DIALOG remains the best means of accessing general archival information, current journals, new books, dissertations and also conferences as covered by the British Library.
- World News Connection, for \$65 a month, or \$90 a profile, is the only means of properly accessing the products of the CIA’s Foreign Broadcast Information Service (FBIS)—they split the world with BBC, which is available through Dow Jones Interactive.

- COPERNICUS is a tool that harnesses the top ten Internet search engines, deduplicates their findings, saves searches, and remembers what you have already seen.
- LEXIS-NEXIS, STN, and other sources are added as appropriate.

2.1.3 Geospatial Shortfalls and OSINT Solutions. Before we discuss private sector offerings with respect to sources of maps & figures as well as commercial imagery, let us take just a moment to contemplate the global situation.

<u>AFRICA</u>	<u>ASIA & PACIFIC</u>	<u>EUROPE</u>	<u>WESTERN HEMISPHERE</u>
Algeria	Bangladesh	Greece	Argentina
Angola	China	Turkey	Bolivia
Djibouti	Indonesia		Brazil
Ethiopia	Kazakhstan		Colombia
Ghana	Kyrgystan		Ecuador
Kenya	Malaysia		Grenada
Liberia	Myanmar		Jamaica
Madagascar	New Caledonia		Mexico
Mozambique	Papua New Guinea		Paraguay
Namibia	Russia		Peru
South Africa	Sri Lanka		Suriname
Sudan	Viet-Nam		Uruguay
	4 Key Island Groups		Venezuela

Figure 22: Global Geospatial Shortfalls Critical to Intelligence

For each of these countries, less than 25% of the country is available in 1:50,000 form, and this is generally very old data. In 1993, for the 69 countries and island groups of concern to the U.S. Marine Corps, there was zero imagery or mapping data available for 22 of the countries; old (10-15 years) 1:50,000 for the ports and capital cities *only* of another 37 of the countries; and complete but very old (over 15 years) coverage for the remaining 10 countries.

In brief, fully 90% of the world is not available in the form of current or dated military maps below the 1:250,000 level, and the U.S. Intelligence Community is incapable of producing such maps for a normal area of operations in less than 60 to 90 days.

We cannot respond to crises with all that we are capable, in the absence of global geospatial information at the 1:50,000 and 1:100,000 level.

At the same time, we must all be conscious of the fact that the Holy Grail for every intelligence professional, automated all-source fusion, will never be possible without a global geospatial database at the 1:50,000 level.

This information is presented in order to suggest that an advance investment is essential in those commercial offerings able to address these requirements.

There is, however, good news.

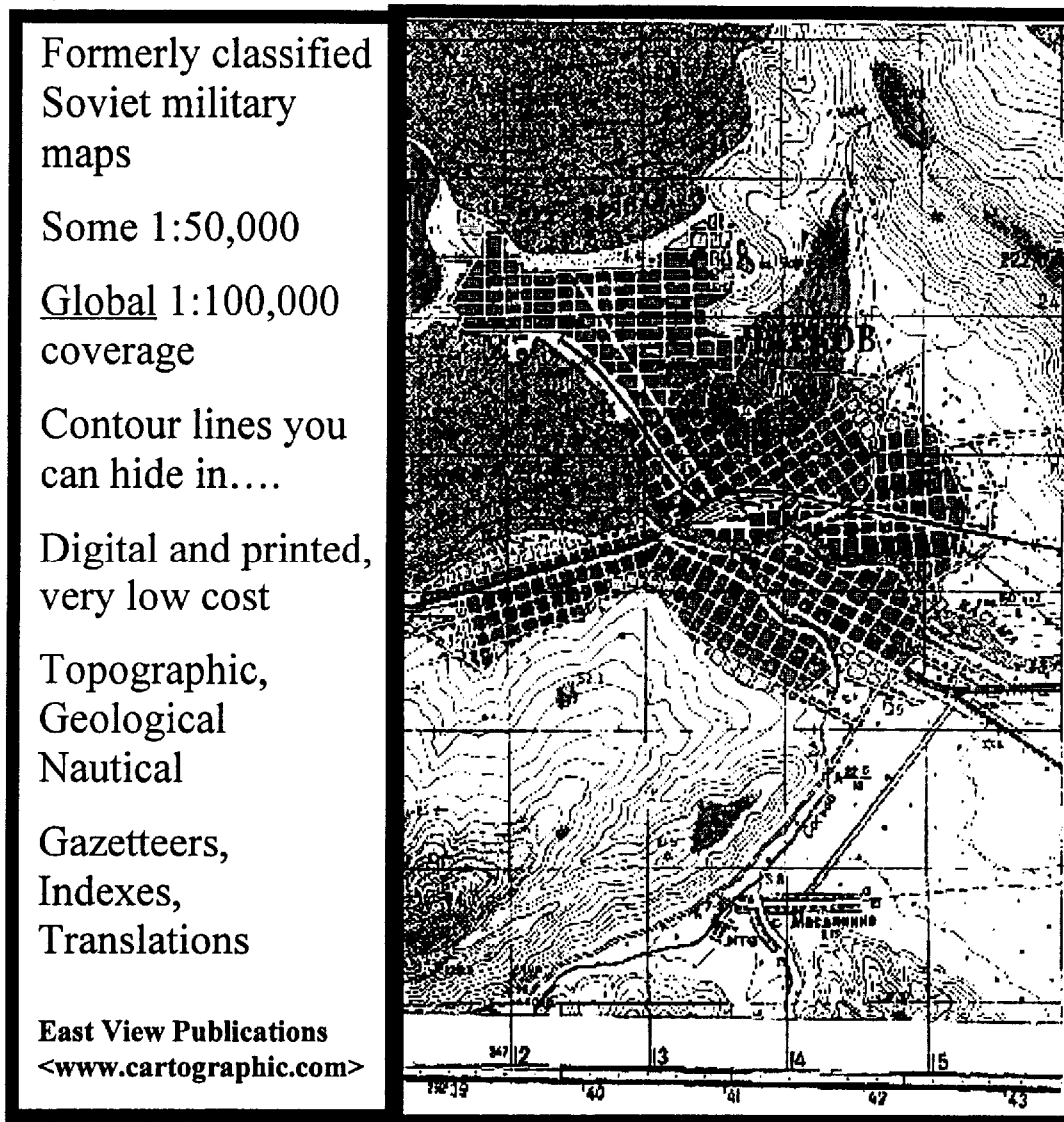


Figure 23: Global Coverage to former Soviet Military Standards¹²

One of the most exciting developments in the geospatial arena has been the relatively recent availability in the private sector of both Russian satellite imagery at the one and two meter levels, and of the entire stock of previously classified “Soviet” military topographic, geological, and nautical maps in both digital and printed form. Above we see a 1:50,000 map from this Soviet source. All of these maps are available, generally within a day or two, through the web site shown here. Although stocks of 1:50,000 are somewhat limited, the entire world—the globe—is available at the 1:100,000 level with contour lines. They had Burundi and this was one of the compelling factors in OSS Inc.’s decisive performance before the Commission on Intelligence. They had Somalia when we did not—they also had the cable car on their maps of Italy when we did not.¹³

There are three critical policy and operational purposes to which 10 meter commercial imagery can be put: the creation of image maps at the 1:50,000 level where fires are coordinated and lives are at risk; the creation of targeting packages for precision munitions; and the creation of three-dimensional interactive nap of the earth and air defense/ingress-egress mission rehearsals. This is so important to both intelligence producers and consumers that we will take each in turn.

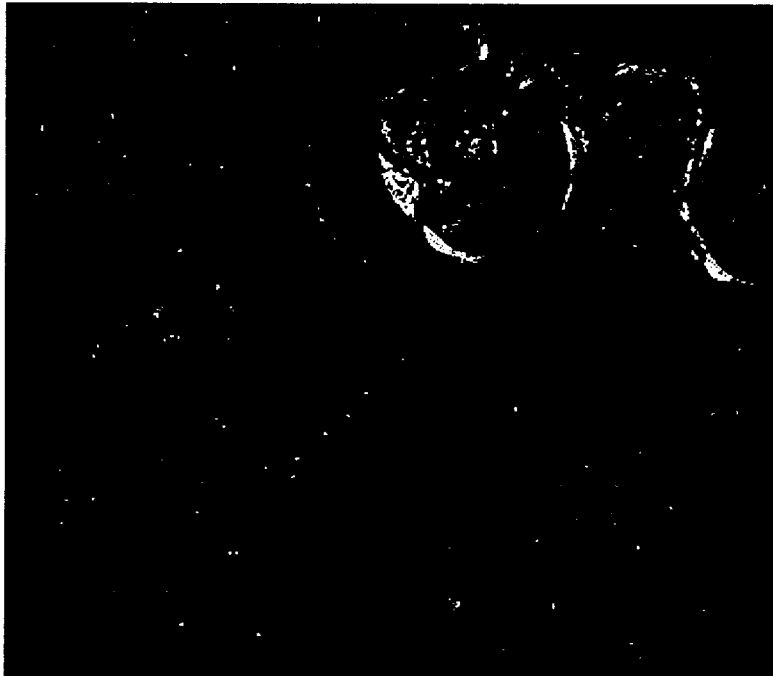


Figure 24: Commercial Image Contribution to 1:50,000 Figure Creation

The creation of 1:50,000 combat figures requires two things: two synoptic images at a different known angle to provide depth, i.e. relief and contours, at a resolution

of 10 meters or better; and a ground control network of points that facilitates accurate ortho-rectification by removing image angle and/or camera focal plane distortions or uncertainties. The number of points depends on the characteristics of the relief - more for highly folded and discontinuous terrain, less for a flat plain, with an average of eight points per 60 square kilometers being the norm. The latter can be obtained from either U.S. national satellites, or from personnel on the ground who use Global Positioning System (GPS) equipment to precisely locate at least eight points visible from space within the 60 by 60 kilometer area. Alternatively, the image maps can be interlaced with the Soviet military maps for which a reasonable but not necessarily perfect ortho-rectification is assumed, and "good enough" 1:50,000 combat figures can be available within days.

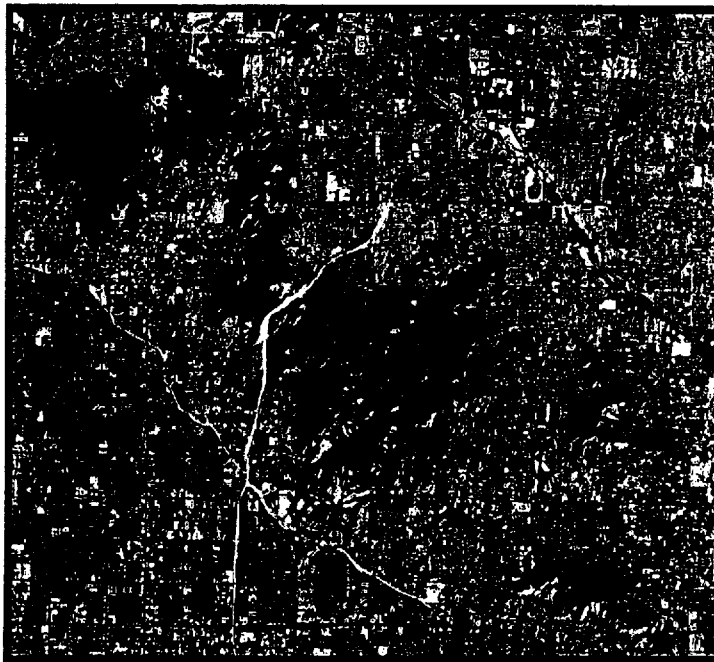


Figure 25: Precision Munition Targeting (North Korean Facility)

The same source can be used to create precision munition targeting packages. During the Gulf War the U.S. Air Force relied largely on this source for its mission targeting. At the time it was found that classified imagery was on an eight day delivery cycle when operational planning was on a three day cycle. While there has been some improvement since then, for "bulk" requirements there is no alternative but to work with commercial imagery.

The third major use for commercial imagery lies with the creation of map of the earth as well as high level three-dimensional *interactive* mission rehearsal programs. These are not only of interest to special operations insertions and extractions, or high-risk attack helicopter runs, but also to normal fighter and attack aircraft operations. Known air defense sites can be integrated, and their "umbrella" of coverage shown in red so that pilots can burn into their minds safer routes. The Wing Commander in Aviano, Italy, then responsible for all flights into Bosnia, is on record as stating that the mission rehearsals created using commercial imagery were responsible for doubling sortie effectiveness.



Figure 26: Mission Rehearsal Scene Using 10 Meter Commercial Imagery

The JOINT VISION ground station developed by the U.S. Air Force is transportable in a single C-130, now takes both SPOT and national imagery directly from the satellites, and is able to feed directly into the Air Force mission rehearsal systems.¹⁴

When the U.S. Army completes their testing of the link between their topographic vans to a JOINT VISION, they will set new standards in what is possible in the way of on-the-fly combat chart production. When combined with geospatial services available from the private sector, discussed in the next section, astonishing open source intelligence is possible.

The greatest myth in both the intelligence community at large as well as the operations community at large, is that classified satellite imagery is essential to the creation of military maps, targeting packages for precision munitions, and nap of the earth mission rehearsal systems. Nothing could be further from the truth.¹⁵

2.2 Open Software. This section avoids discussion of specific products because they are as yet not suited for “plug and play” end-user adoption.

2.2.1 Software Functionalities. These are the *functionalities* that we require.

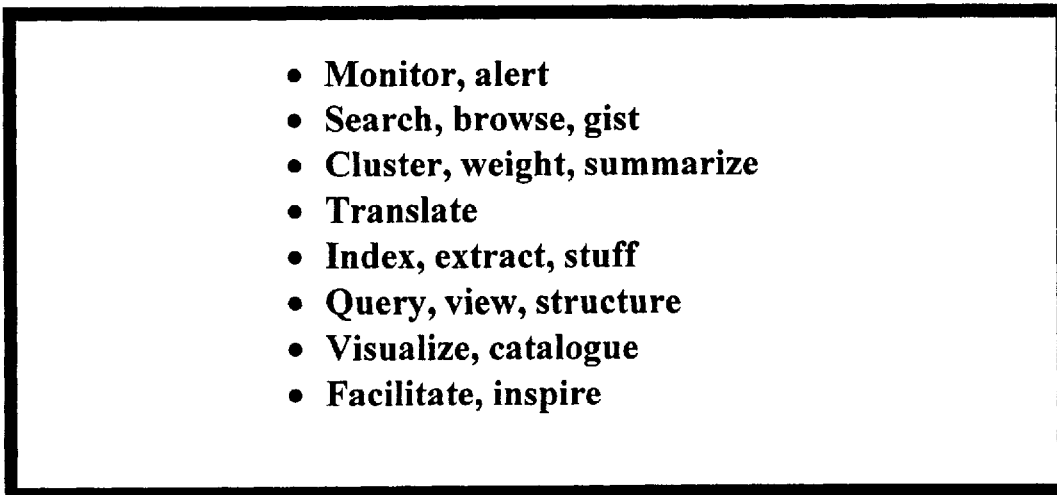
- 
- **Monitor, alert**
 - **Search, browse, gist**
 - **Cluster, weight, summarize**
 - **Translate**
 - **Index, extract, stuff**
 - **Query, view, structure**
 - **Visualize, catalogue**
 - **Facilitate, inspire**

Figure 27: Needed Software Functionalities

There have been significant strides forward in information processing, and especially in retrieval software and visualization software.

However, most software pieces—and certainly all those intended for scalable operations—are *not* ready for “plug and play” initiatives. They require costly, painful, and often very disappointing starts and stops before finally coming together adequately. The industry continues to build software in isolation from reality. We have not yet found a software offering that was designed in relation to real data sources and real data outputs while also being conscious of the end user’s desire need for something that will simply install into their server.

The continuing lack of standards, in something as simple as htm versus html file endings for incoming open source, or search & retrieval protocols so that one profile can be used with multiple sources, or the lack of “date of information” and “date of publication” search fields on the Internet, all constrain open source collection and production as well as all-source analysis.

To be blunt, commercial open software usually delivers less than it appears to promise, and perhaps a tenth of what the end-user expects. Apart from installation and inter-operability issues, the biggest problem we see every day is the training burden—either training and documentation are inadequate, or training is so complex as to make it highly unlikely that training be undertaken or remembered if it is taken. The industry has not yet mastered transparency and intuitive interfaces.

This problem is further compounded by the inadequacy of in-house systems administrators, at least within the U.S. government. Perennial issues include:

- Mainframe era staffing—don’t understand PCs, servers, and networks
- One deep—rarely have the time to deal with “one of” applications
- Obsessed with security and structured database approaches—can’t understand “unstructured text” and imagery or object databases or HTML bundles.

Software is, however, easily a third of the solution, and putting the right pieces together is part of being able to create open source intelligence.

2.2.2. Data Visualization

The figure on the next page is a screen from one of the more popular visualization applications available. It is highly recommended by Scotland Yard’s Open Source Intelligence Unit.

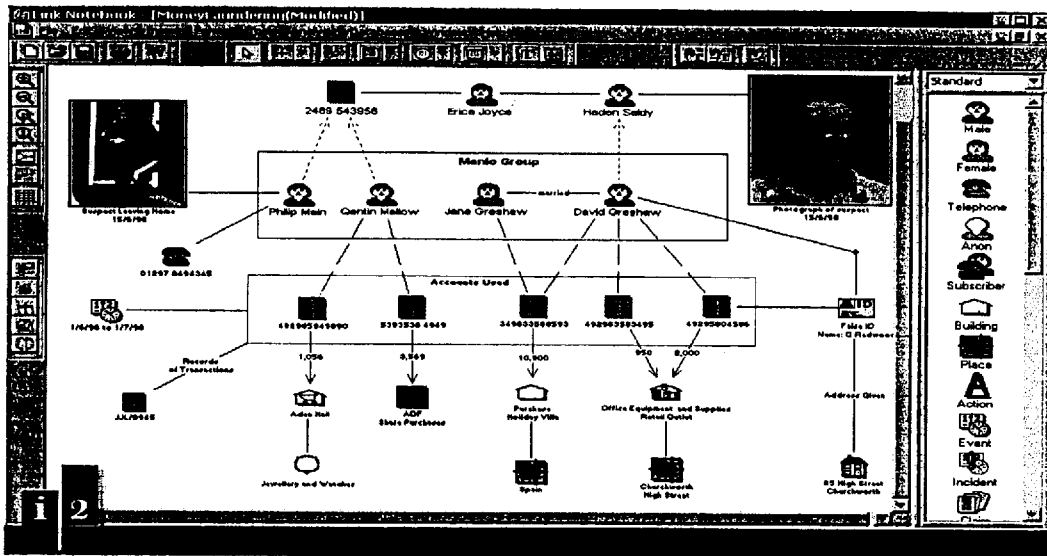


Figure 28: Analysts Notebook -- Link Analysis -- <www.i2inc.com>

2.2.3. Data Exploitation

Here is another screen, from a complementary product.

Figure 29: Private Sector Software Offering -- <www.memex.com>

What one might emphasize here is the integration of the search, retrieval, and exploitation functionalities.

Our experience has led us to believe that there is now a disconnect between the emerging software capabilities of the private sector, and the increasing inadequacy of the government systems administration personnel. For this reason, we believe that the most successful software offerings will be those that can be exploited on a fee for service basis through direct web access and without any installation being required. We also believe this implies a marketplace for secure data warehouses where specific kinds of open source data can be brought together and securely stored, with full copyright compliance, or exploited as appropriate. In short, we expect the government to hire the people, and the private sector to manage *both* the bulk of the data, including classified data, and the bulk of the processing.

2.3 Open Services. It is important to stress that unlike sources or software, services are essentially about human expertise, acquired over decades, being applied on your behalf in real-time.

2.3.1 Data-Oriented Services. At the end of the day, open source intelligence is about smart people putting smart words down on paper. Before we get there, however, we need lots of smart people doing smart things in collection.

- **Online Searchers**
 - **Source-centric/each system unique**
 - **Subject-matter competence/learning curve**
 - **Foreign language competence/full access**
- **Document Retrieval**
 - **Gray literature source access**
 - **Copyright compliance**
 - **Digitization**

Figure 30: Data-Oriented Services with Very High Human Value-Added

The average information broker is skilled at one major online system, and has local subject-matter experience. A proper effort may often require the exploitation of a number of different online systems, each with their own arcane command languages. It may also require specific subject-matter competence such as familiarity with nuclear terms; and it may benefit significantly from foreign language competency so as to permit the very rapid assessment of original materials in a language other than English.

Document discovery is much more complex than simply discovering a document through an online listing. Our experience has shown that the bulk of the really valuable documents are not in electronic form and not listed online. They comprise what is known as “gray literature”. Gray literature is literature that is legally and ethically available, but produced in limited quantities and generally not available outside a limited circle. School yearbooks, academic pre-prints, dissertations in progress, and think tank papers generally fall into this categorization.

Document delivery can be more complex than receiving a fax, if one wishes to be assured of copyright compliance, authority to redistribute the material, and an ability to digitize it and store it for more than ninety days.

2.3.2 Human-Oriented Services. Human beings applying knowledge on your behalf are uniquely effective.

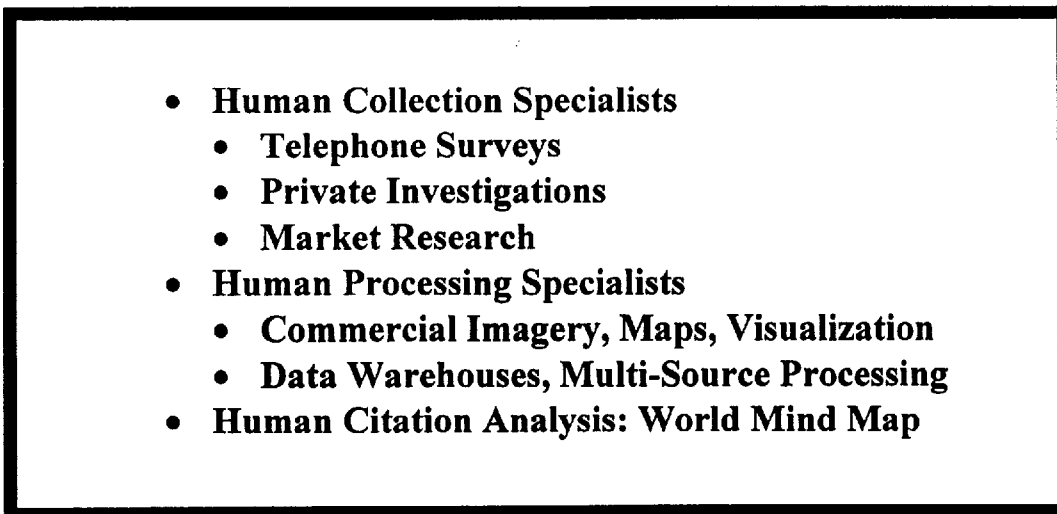
- 
- **Human Collection Specialists**
 - **Telephone Surveys**
 - **Private Investigations**
 - **Market Research**
 - **Human Processing Specialists**
 - **Commercial Imagery, Maps, Visualization**
 - **Data Warehouses, Multi-Source Processing**
 - **Human Citation Analysis: World Mind Map**

Figure 31: Human-Oriented Services with Very High Value-Added

Telephone surveys are an art form. Knowing which professional associations to call; knowing what job titles to ask for; knowing how to create a calling matrix that gets the right bit of information from the right person, without revealing the whole of the question to any one person—doing all this without violating any old or new espionage laws—these are valuable skills.

Private investigators and market researchers are both under-appreciated and oversold. They can do a great deal, yet your average government organization would never consider out-sourcing to them those things they can do better than a government employee—or those things that might not get done at all. At the same time, they have a narrow range of expertise, and cannot be considered open source intelligence producers in the sense of this report.

Human processing specialists can extract extraordinary amounts of information from commercial imagery, and even merge commercial imagery and selected classified information in ways that the classified imagery analysts cannot even begin to understand.

Citation analysis is the fastest way to learn stuff. More on that further on.

2.3.3 Information Brokers

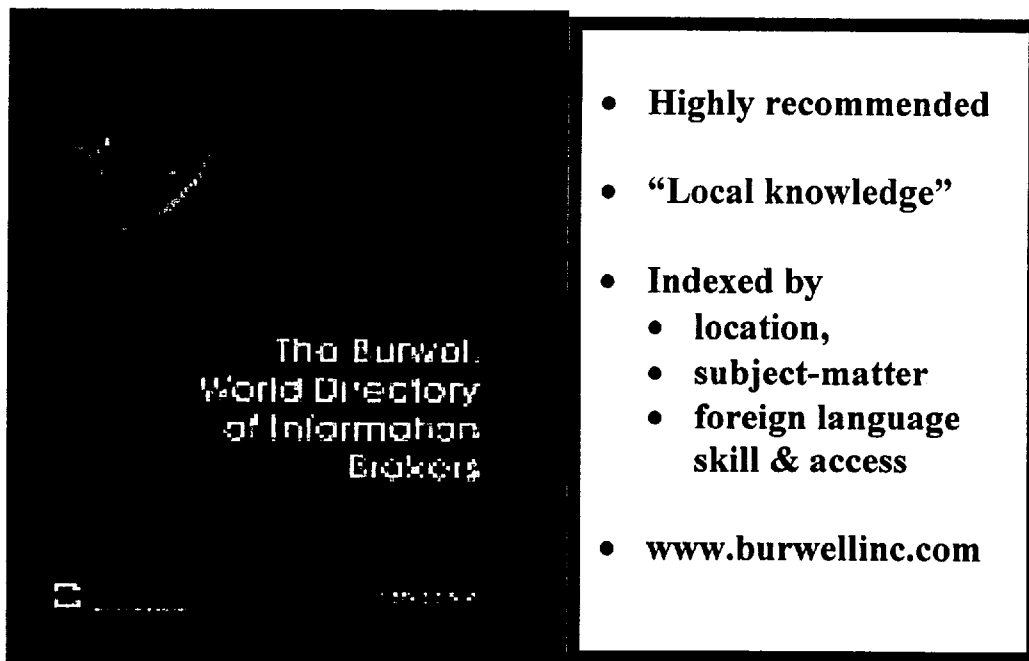


Figure 32: *The Burwell World Directory of Information Brokers*

The directory, *The Burwell World Directory of Information Brokers*, is how each intelligence professional should spend their first hundred dollars when they get around to creating an open source intelligence process.

It is indexed by geographic location, subject-matter and database expertise, and—at the suggestion of OSS Inc. and beginning in 1995—by foreign language and foreign language competency. This is “Ref A” for any global inquiry.

Perhaps more importantly, its publisher, Ms. Helen Burwell, is in a literal sense the world’s most authoritative source on what the individual information broker’s true competencies are (the stuff that’s not in the book), and how best to mix and match different brokers and different approaches.

Each broker, in turn, can serve as an agent in identifying and contracting with selected other local capabilities and overt sources of specific kinds of information.

2.3.4 Geospatial Visualization

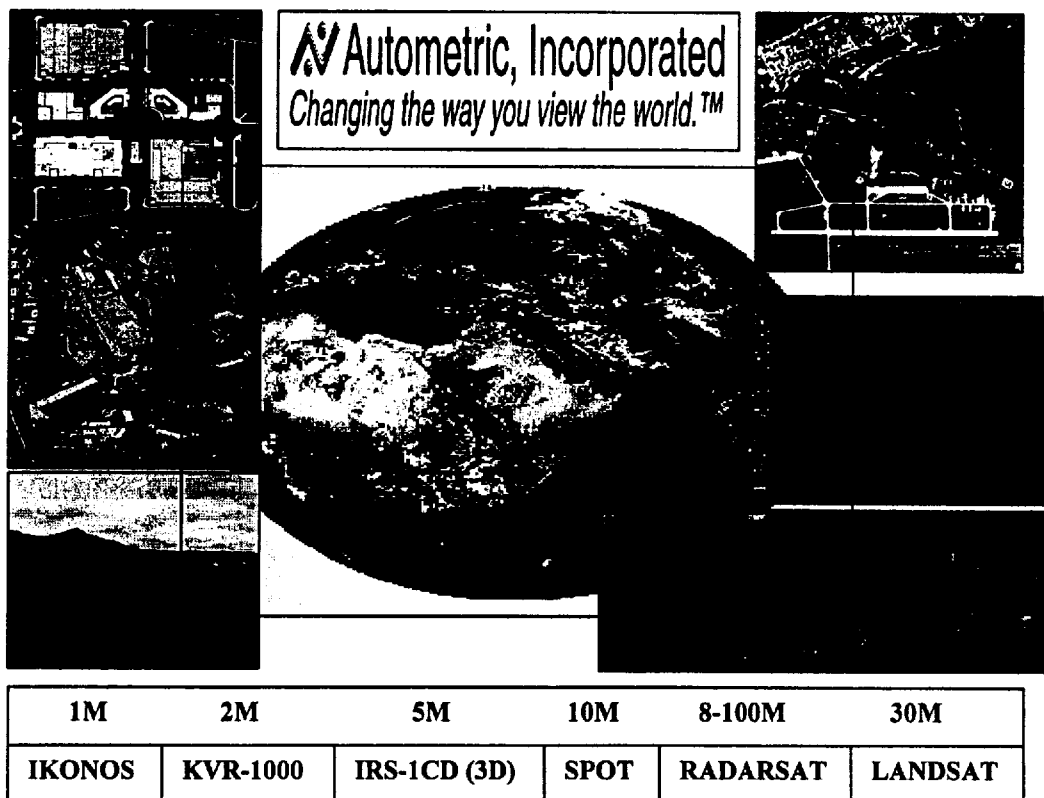


Figure 33: Geospatial Visualization and Multi-Source Commercial Imagery

The average commander, staff officer, and intelligence analyst is inadequately familiar with the full range of commercial imagery sources that can be brought to bear on an intelligence requirements. They are also generally unfamiliar with the exceptional capabilities that exist in the private sector for mixing and matching multi-source commercial imagery to achieve specific objectives. Finally, they are usually unaware of the fact that the private sector is fully able to integrate classified national imagery and geospatial data with commercial imagery, and that the private sector generally has superior (that is to say, current) information technology processing software and equipment including *workable* virtual reality and efficient three-dimensional conversion software.

Apart from the simple availability of commercial imagery, addressed previously, is the larger issue of how one applies deep knowledge about alternative sources of commercial imagery, and deep knowledge about advanced information technology that permits both the integration of disparate sources, and the extraction of information impossible to visualize without the use of advanced information technologies.

At the center of the newest revolution in national and defense intelligence is the emergence of a new visualization metaphor for data, one that is firmly grounded in geospatial reality. This new global visualization metaphor permits the management of massive amounts of multi-media data inside of a geospatial architecture—a virtual reality—that at one stroke makes all-source data fusion a reality, and also give the intelligence product a "look and feel" that is an order of magnitude improvement of anything the policy-maker, commander, and staff have been accustomed to in the past.

This preceding figure shows different kinds of imagery, at levels of resolution varying from two meter to thirty meter, and using different kinds of imagery, from panchromatic to multispectral to all-weather radar. Anyone who is not operating at this level of sophistication is severely disadvantaged.

- 2 meter imagery is available today from the formerly classified Russian satellite system. U.S. one meter imagery will probably become a reality by around 2000, but it will be one to two years before it can do global coverage.
- 5 meter imagery is available from the Indians, but they only have one satellite so it is limited in both coverage and capability (ability to take two looks necessary to create contour perspectives).

- 10 meter French imagery, *the industry-strength industry standard*. This is the only commercially-available system with multiple satellites, a global network of effective ground stations, multiple years of global coverage in the archive database, and the ability to provide two day revisitation.
- 8-25-100 meter Canadian radar imagery, a non-literal source, requiring different training from the electro-optical systems but uniquely valuable for its ability to collect in all-weather and at all hours. It's standard setting is at 25 meters, but it can be tasked to 8 meters.
- 30 meter multispectral U.S. imagery, this also approaches industry strength, and is a widely appreciated source.

The hard truth is that the U.S. Intelligence Community has only done minimal planning for commercial imagery as a major source, with the result that both the National Reconnaissance Office (NRO) and the National Imagery and Mapping Agency (NIMA) have created a legacy system that is unprepared for adjusting to the wealth of commercially-available imagery and related geospatial data. There are also major trade-offs that have heretofore been studiously avoided in planning and programming discussions. For instance:

- TRANSMISSION TIME
- ELECTRONIC STORAGE
- COMPUTER PROCESSING TIME
- COST

In each of these cases, studies originating within the office of the Vice Chief of Staff of the Air Force (where EAGLE VISION and JOINT VISION are based), have documented the extraordinary order of magnitude differences between the requirements associated with national imagery (1 meter and below) versus commercial imagery sources in the 2-30 meter range.

The fact is that 10 meter imagery is "good enough" for the three major military requirements: combat charts, most munitions targeting,¹⁶ and aviation/special operations mission rehearsal, but the operational consumer has been ignorant of the options and too willing to permit the U.S. Intelligence Community bureaucracy to carry on with business as usual. As commanders, staff, and-indeed-intelligence analysts begin to realize that they can get a square kilometer anywhere in the world for roughly \$10.00 to \$40.00 depending on resolution, there should be a revolution in how we approach the enormous potential of global geospatial imagery and data from multiple commercial sources.

2.3.5 Citation Analysis. We've mentioned citation analysis. This is perhaps the single least exploited capability in the open source world. It continues to astonish when one finds Directors of Research for major think tanks and heads of branches within intelligence organizations who have never heard of the *Science Citation Index* or the *Social Science Citation Index*, both flagship publications of the Institute of Scientific Information (ISI) based in Philadelphia, Pennsylvania.

With these, both available online through DIALOG but best exploited through ISI's in-house software, one can identify current authorities—based on being cited rather than being prolific—on almost any topic. One can also, using an older reference known to be on target, rapidly identify everyone who has ever cited that reference, and in this way quickly identify current thought leaders, recent publications, and “centers of excellence” in specific areas.

Something that is only available through ISI itself, and a related company with access to the same master data, are citation *maps* such as illustrated below. They are working to also show these as geographic terrain. Such depictions are extraordinarily useful in identifying centers of excellence around the world and not usually cited in English; in identifying the leaders in specific sub-disciplines and especially those who branch multiple disciplines; and finally, in identifying emerging products and capabilities.

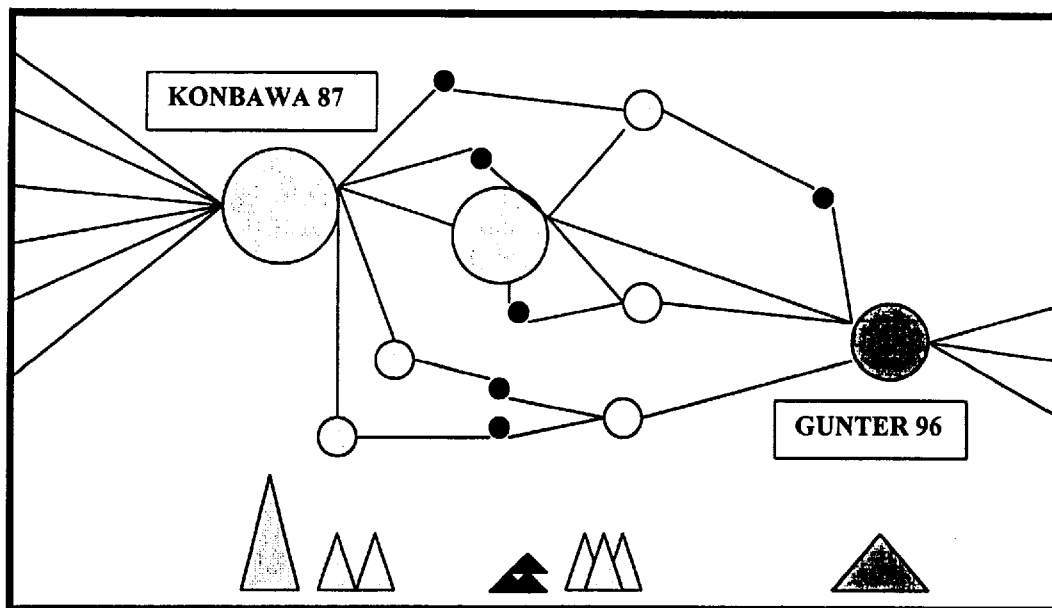


Figure 34: Citation Analysis

2.4 OSINT Overview. To conclude this orientation on open sources, software and services we will address some OSINT “issue areas”; some of the “rules of the game” that we have identified through experience; the reality of the vastly over-rated Internet; and the nature of OSINT as a process, finishing with an illustration of an integrated OSINT concept.

2.4.1 OSINT Issues Areas. Over time we have identified four major “issue areas” that are consistently of concern to our clients, or misunderstood by our clients.


- 
- **Operational Security**
 - **Copyright Compliance**
 - **Foreign Language Coverage**
 - **Source Validation**

Figure 35: OSINT Issue Areas

Those who have not actually served within an intelligence or defense community can never appreciate the deep concerns about operational security and the need to conceal the very fact that the question is being asked at all. This is a normal concern for intelligence and defense professionals, and also for wise business professionals. Addressing these concerns up front, and providing assurances with respect to how the process will not relate the question to the client, are important aspects of success in marketing open source intelligence.

Copyright compliance is harder. Governments are accustomed to ignoring copyright, or classifying everything so their violations are not discovered. It *is* possible to comply with copyright, even though the law is years behind electronic practices. It is worth doing and will pay dividends later.

Foreign language coverage is very weak in the Anglo-Saxon world. We need to provide incentives to the online community to buy, digitize, and offer electronic access to significant quantities of foreign language information.

Few private sector information professionals, in our experience, routinely address source bias, context of coverage, and other source validation issues.

2.4.2 OSINT Rules of the Game. There are myths, and realities, and rules of the game.

- **80% of what you need is *not* online**
- **50% of what is not online has not been published at all**
- **60% of what you need is not available in English**
- **90% of the maps you need do not exist**
- **90% of the geospatial data you need is in private sector**
- **80% of the information overall is in the private sector**

Figure 36: OSINT Rules of the Game

Standing up the Marine Corps Intelligence Activity, at a cost to the U.S. taxpayer of \$20 million, we learned the hard way that 80% of what we needed to produce intelligence was neither within the classified systems, nor within the commercial online systems.

And of what we need that is not online, roughly half of that has not been published at all—one needs to go directly to humans on the ground.

We've already mentioned that 90% of the maps needed for the planning and execution of global operations are not available—but fortunately commercial imagery can resolve this deficiency within a few years, at a cost of roughly \$250 million a year, funded by the U.S. taxpayer on behalf of all governments.

The center of gravity for national intelligence is now in the private sector. Governments need to learn how to leverage this valuable private knowledge, and businesses need to learn how to create intelligence from open sources.

2.4.3 The Reality of the Internet. The Internet is both good and bad. The bad news first.

- **COSPO (USA) Survey: roughly 1% of Internet is real content, roughly 50 great sites, 500 good sites--the rest is pornography and opinion**
- **Internet is a cream puff in comparison to the kind of rich content/value added represented by commercial online services with editors/filters**
- **MCIA/Other Experience: Internet devours analysts--they get lost or they get addicted, either way their productivity is cut in half**

Figure 37: The Really Bad News about the Internet

The Internet is grossly oversold. A formal study by the Community Open Source Program Office of the U.S. Intelligence Community determined that less than 1% of the "content" of the Internet is actually substantive. They found only 50 very high-value sites and 500 good sites. The rest was pornography and opinion. Granted, this was in 1996 and the Internet is growing exponentially, but it is a useful cautionary benchmark.

The Internet is thin soup indeed when compared with the robust value-added offerings of a commercial online service such as DIALOG or LEXIS-NEXIS. Apart from the fact that vast quantities of substantive information have been carefully acquired, digitized, indexed, and placed in a relatively easy to use environment where search and retrieval functions are standardized, commercial online services provide something the Internet does not: time value. You pay cash and save time.

The Internet *devours* analysts. They simply disappear. On balance, giving analysts direct access to the Internet may well be the equivalent of giving them an

open bar during working hours. The Internet is a serious productivity drain, and it merits comment that search skills are different from analysis skills.

The good of the Internet is *quite* good. It is an extremely useful environment for collaborative work and for information sharing. This however, has its limits, as it only applies to the USA and with much tighter limits, to very educated and well-off Europeans, Australians, and Canadians. In Africa the Internet does not really exist. In Asia and the former Soviet Union it is severely handicapped.

- **Internet is extremely useful as a collaborative work environment, and for information sharing**
- **Internet has its uses (see OSINT HANDBOOK)**
 - **Indications & Warning (Tiananmen, Coup vs. Gorby)**
 - **Cultural Context (Bosnia, Islam, Indians in Mexico)**
 - **Basic Research (card catalogues, lists, web sites)**
 - **Science & Technology (surprisingly good)**
 - **Spotting & Assessment (trolling for potential assets)**
- **Internet will explode over time—early days yet**

Figure 38: Internet Utility and Potential for Intelligence Purposes

The Internet does have its uses for intelligence, and these are discussed in the *Open Source Intelligence HANDBOOK* as published by the Joint Military Intelligence Training Center within the Defense Intelligence Agency. The Internet *can* contribute—within the limits of bias, time, and skill—to indications & warning, cultural contextual understanding, basic research, science & technology collection and even spotting and assessing potential agent candidates.

The Internet is, above all, an “out of control” resource that is growing exponentially and is likely, in ten years time, to be the single most overwhelming command & control network in the world, linking each and every individual to each and every piece of open source information that anyone cares to offer up, either for free or for fee—and to all other individuals who join this network.

2.4.4. **OSINT as a Process.** We end this rather large segment, this overview on open sources, software and services, by noting that open source intelligence is a *process* rather than a product.

- **DISCOVERY: Know Who Knows**
 - Just enough from just the right mix of sources
- **DISCRIMINATION: Know What's What**
 - Rapid source evaluation and data validation
- **DISTILLATION: Know What's Hot**
 - Answer the right question in the right way
- **DELIVERY: Know Who's Who**
 - It's not delivered until right person *understands*

Figure 39: The OSINT *Process*

This process requires human as well as automated knowledge about “who knows” and how well do they know it.

It requires an ability, far from maturity in technology, to rapidly evaluate sources and validate data.

It requires an ability to know what the client *really* wants, so as to be able to answer the right question, in the right way.

Finally, it requires an ability to *communicate* the intelligence in such a way that a compelling presentation leads to action or at least *understanding*.

OSINT is inherently a process that integrates human expertise in requirements, collection, and analysis, with deep knowledge of sources, and some advanced information technology applications.

2.4.5 **Integrated OSINT Concept.** The figure below illustrates the OSS concept as it is being realized in The Information Merchant Banking System™. It is still evolving but is off to a good start since it was initiated in February 1998.

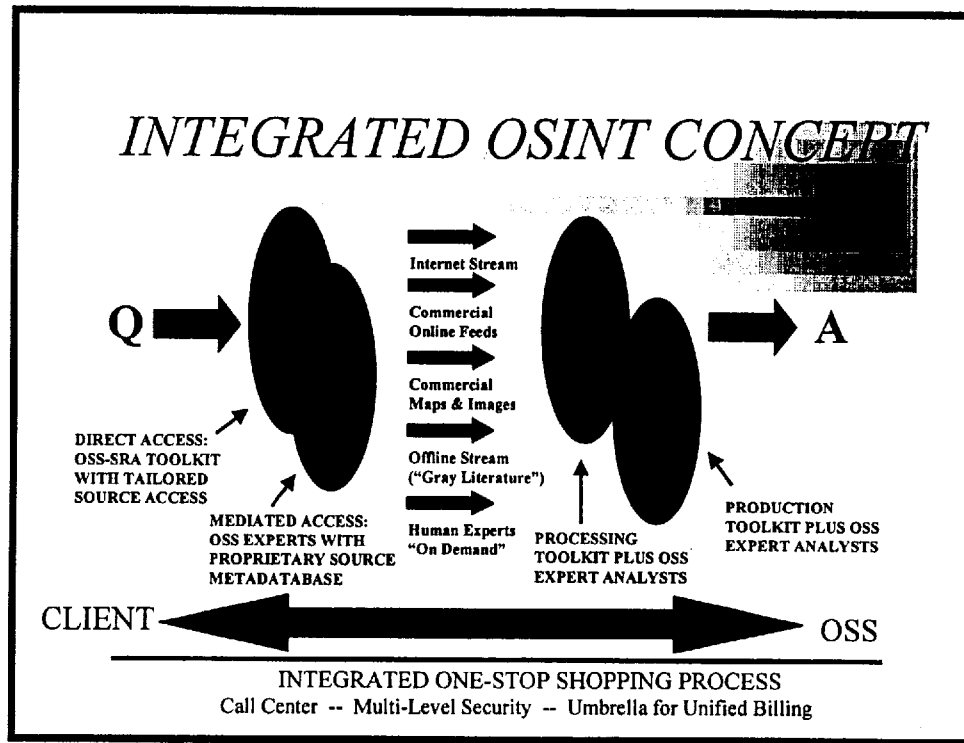


Figure 40: Integrated OSINT Concept

We are migrating our expanded offerings to the Web, and will shortly be offering anonymous access to both an Open Source Marketplace™, and anonymous access to our various *Daily Intelligence Briefs* as well as our other offerings.

This process can be replicated by anyone that wishes to, although we suspect that most would find it too troublesome to put together as we have. In developing this, we have been quite careful, going at full speed, to find and hit every single pothole on the information superhighway.

In all of this process, there is no element more important than the feedback loop, to the point that we have institutionalized an electronic means of allowing the collection analyst, the production analyst, and the consumer to embed comments into the product itself.

3.0 OSINT AND COLLECTION MANAGEMENT

3.1 General Uses of OSINT. It is helpful to remember that collection management is about *targeting* specific resources against specific individuals, facilities, or signals. Collection management cannot take place in a vacuum. Indeed, when classified capabilities are run in “vacuum cleaner” or indiscriminate mode, two things happen: expensive resources are placed at risk to collect information that probably is not classified to begin with; and analysts are overwhelmed with reporting of dubious value. OSINT can play a very important role in optimizing collection management.

- **TIP-OFF**
 - **Wire Services, Jane’s**
- **TARGETING/CONSERVATION**
 - **Narrow the field**
- **CONTEXT/VALIDATION**
 - **Signal or image context, validate informants**
- **COVER**
 - **Protect classified sources & methods**

Figure 41: OSINT Support to Collection Management

Although it is counter-intuitive, a careful examination of defense intelligence in 1995 discovered that more often than not, it is open source that tips off classified collection management. Time after time, an item in a wire service or an article in Jane’s inspires a classified collection tasker.¹⁷

Open source is not being used properly, at least within the U.S. Intelligence Community, to target classified resources. This is especially true of the clandestine service. Ultimately this will be the greatest contribution of open sources: to provide sufficient information about less difficult targets, and enough information about more difficult targets, so as to permit the narrow-casting of classified capabilities.

The law enforcement community, and especially the Royal Canadian Mounted Police and EUROPOL, are at least a decade ahead of the U.S. Intelligence Community with respect to using open sources to provide contextual information for judges and juries, and to validate informants.

Finally, and this is perhaps well enough along, open sources, and especially commercial imagery, are providing very useful and “good enough” open intelligence to those with whom we cannot share “the best” stuff.

3.2 OSINT as a Foundation. Spies are necessary and admirable elements of a proper national security community. They are most effective, however, when managed as part of a true all-source collection and production process.

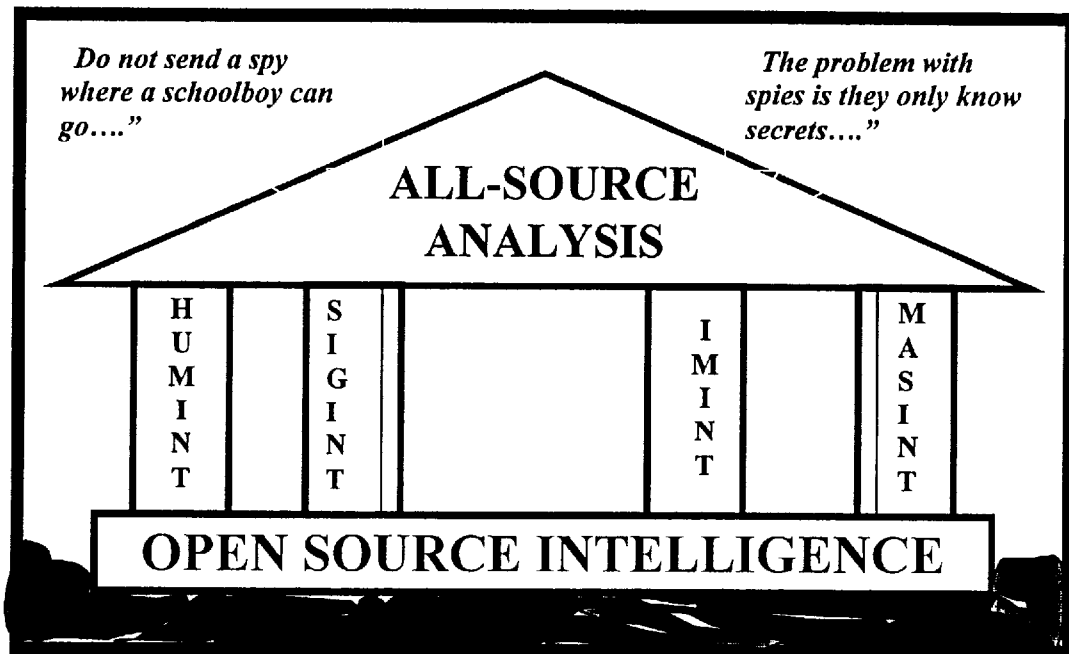


Figure 42: OSINT as the Foundation for All-Source Intelligence

It is foolish and contradictory to use spies for tasks that can be accomplished by scholars, legal travelers, or what have you.

It is also foolish to have spies that do not know the difference between a secret and an open item of information.

Finally, it makes no sense at all to spend a great deal of effort piecing together analysis using only classified sources, when the bulk of the work can be had for the price of a dissertation from the Sorbounne.

Open Source Information is “the good earth” upon which an Open Source Intelligence foundation can be built—a foundation strong enough to support the four classified pillars of traditional intelligence, pillars upon which rest the all-source analysis endeavor.

Neither classified collection, nor classified production, can be considered “all-source” unless it first masters and then fully exploits the open source world.

3.3 The Changing Collection Paradigm

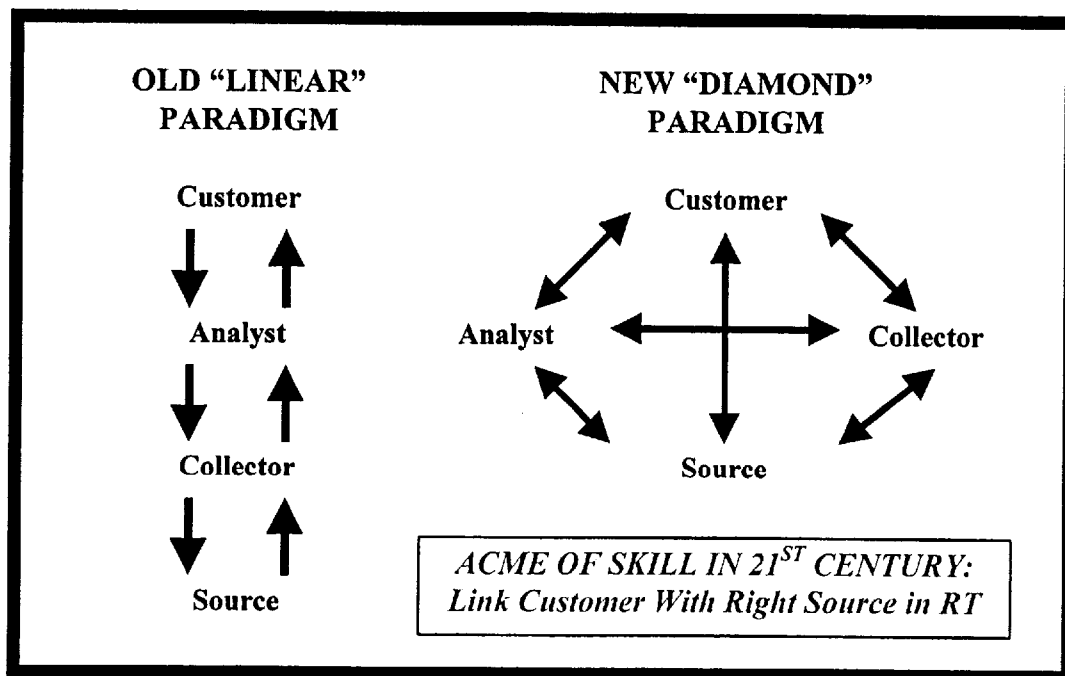


Figure 43: The Changing Collection Paradigm

The old “linear” paradigm is no longer fully effective. Under this old paradigm, the customer went to the analyst; if the analyst could not answer off the shelf, then the analyst went to the collector; if the collector did not have something collected but unprocessed, then they went to the source.

What few will admit is that all too often, the source would go read open sources, pretend they had a third cousin in the appropriate ministry, and turn this over as purported gossip or insider information. The case officer, working from low burn time files and not reading the open source literature, would not realize they had

been had, and back up the chain it would go, as WNINTEL NOFORN NOCONTRACT....open source.

Under the new “diamond” paradigm one encounters both a vastly enlarged universe of overt sources that can be of direct service to both the analyst and the customer; and also the need, in dealing with complex issues, for direct contact between the customer and the collector, and sometimes between the customer and a covert source, even if in the form of written messages.

4.0 OSINT AND ALL-SOURCE ANALYSIS

4.1 The Changing Analysis Paradigm. In both government and business, the role of the analyst is changing. The traditional analyst, who at least in government has generally been isolated and been asked to work with source material that is delivered to their desk, in order to produce intelligence that is taken from their desks and given to clients they may never meet (indeed, clients who in all likelihood will never read their products at all), is a thing of the past.

The preceding figure has much to offer the modern analyst as well as the modern collector, and reflects a fundamental shift away from structured institutionalized and largely secret intelligence, toward a new international networking form of intelligence in which most of the sources—and perhaps even most of the analysts—are not full-time government employees nor do they even have a secrecy agreement (in the case of sources) or a clearance (in the case of analysts).

4.2 Changing Role of the All-Source Analyst. As we enter the 21st Century, the modern intelligence analyst must move away from their insular and self-centered practice of focusing on inanimate all-source reports that have been harmonized into text, and begin focusing on people and interacting with people.

- The modern analyst must be able to identify and manage a network of overt sources; and must be able to manage the funds with which to compensate those overt sources as well as various providers of open source services.
- At the same time, emboldened and enlightened by a superior contextual understanding established through open sources, the modern analyst must become a much more aggressive, critical, and specific manager of classified collection capabilities (or sales collection, in the case of business).

- Finally, the modern analyst must be able to fully integrate themselves into the client’s working environment, both in terms of providing a first assessment of the open sources reaching the client, and also in terms of being sensitive to the client’s needs for unclassified intelligence.¹⁸

4.3 OSINT and Multi-Level Analysis. Just as the role of the analyst must change, so must their focus.

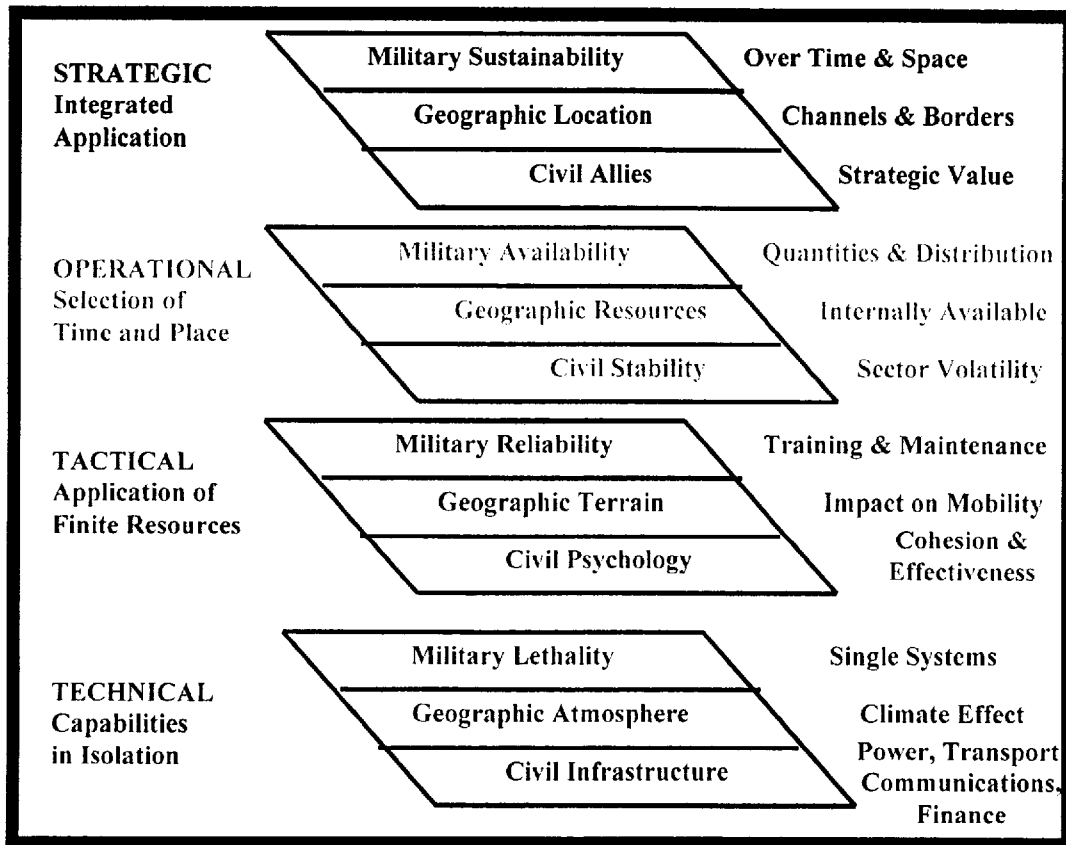


Figure 44: OSINT and Multi-Level Analysis

The modern analyst must move dramatically past the traditional practices of “cutting and pasting” subject lines, maintaining files largely useless to anyone, and being primarily a “stuckee” for point papers or taskers having to do with the area arbitrarily assigned to the analyst, not because they are expert in that area, but because “somebody has to handle the Balkan questions.”

The modern analyst must be able to impact on major decisions. Such decisions includes strategic ones having to do with long-term investments; operational ones relating to choosing the time and place of confrontation with others; tactical questions of exactly what tools and tactics to use to win the engagement; and finally, technical issues relating to the actual use of whatever capabilities the decision-makers are employing. Open sources have much to offer in all these areas.

Above all , the modern analyst can no longer be allowed to produce “situation reports” that are nothing more than a classified version of the news, or compendiums of information that are relatively useless. The modern analyst has to get back in the business of answering important questions in real time. This must include the ability to distinguish between levels of threat, and to formulate strategic generalizations.

4.3.1 OSINT and Threat Analysis

Here is a real world example of how the threat changes depending on the level of analysis.

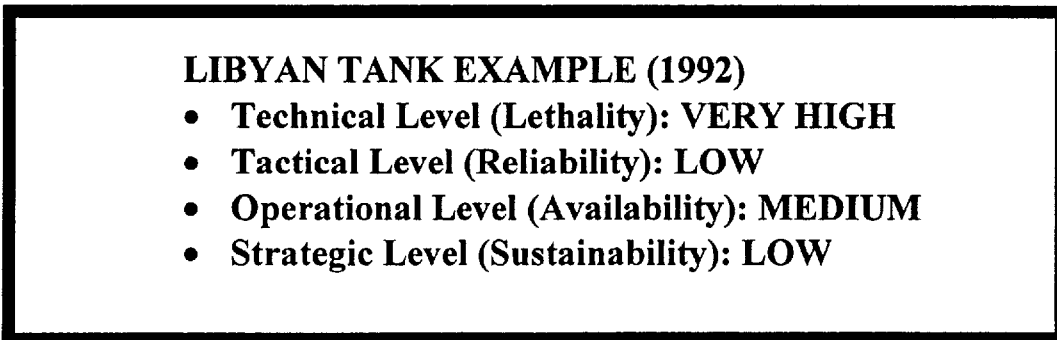


Figure 45: Threat Changes Depending on the Level of Analysis

At the technical level, which is where the U.S. Intelligence Community traditionally starts and stops, the Libyan tank threat in 1992 was “very high” because they had lots of Soviet T-72 tanks, then considered the best.

However, at the tactical level, when one took the time to consider their reliability, and especially the lack of training of the crews, the cannibalization of some tanks for parts to keep others operational, and the storage of most of the tanks in the open, the threat readily dropped to low.

At the operational level, where one is concerned with availability, the threat rose to medium because of the numbers of tanks and their relative distribution. At the strategic level, where sustainability is of paramount importance, the threat dropped to low.

We can no longer afford to design and build all our systems on the basis of intelligence analysis that starts and stops with the technical level.

OSINT can make significant contributions to formulating threat hypotheses at each level of analysis.

4.3.2 OSINT and Strategic Generalizations. At the same time that we improve our understanding of threat levels, we need to be able to present our policy-makers, commanders and their staffs with strategic generalizations that are very useful in affecting long-term and very expensive acquisition programs.

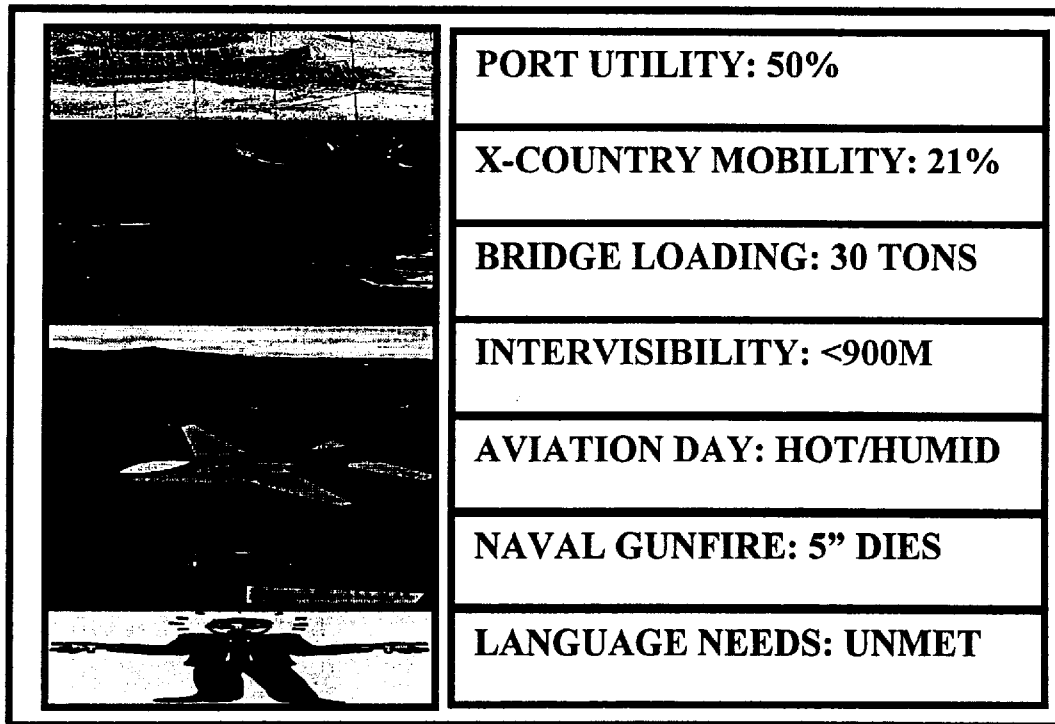


Figure 46: OSINT and Strategic Generalizations

Fully half the ports where we are most likely to go will not permit Navy ships to get close enough for pier-side offload.¹⁹

Cross-country mobility is “zero” in 79% of the countries of interest, and bridge-loading limitations average 30 tons.

What about line of sight distance? Under 900 meters in all but six countries.

Or aviation temperatures. The U.S. Navy designs for a warm day. The expeditionary environment is fully seven degrees hotter and much more humid.

The U.S. Navy 5” is out-gunned and useless almost everywhere, at the same time that the carriers insist on staying 200 NM from the shore. This has two practical effects: when carriers are not available to support an Amphibious Ready Group, the Marines are vulnerable to shore-based anti-ship missiles; when the carriers *are* available, their stand-off posture and prevailing temperatures (with high humidity) limit the jets to five minutes over the battle area.

And then there is language—language deficiencies are routine across the board, including military police, engineers, and of course, intelligence.

5.0 OSINT AND COALITION OPERATIONS

5.1 **Intelligence Upside Down.** Nowhere does OSINT prove itself more valuable than as a means of fostering a common view of the area of operations, and as a means of nurturing information-sharing in a coalition environment.

“...the concept of UN intelligence promises to turn traditional principles on their heads. Intelligence will have to be based on information that is collected primarily by overt means, that is by methods that do not threaten the target state or group and do not compromise the integrity or impartiality of the UN.”

Hugh Smith as cited by Sir David Ramsbotham

Figure 47: OSINT and Coalition Operations

This quotation, for an article on “Intelligence and UN Peacekeeping” in *Survival* (Autumn 1994), has become a standard capstone statement.²⁰

The reality is that coalition operations *demand* not only a foundation comprised of open source information and intelligence, but may even be limited by choice as well as circumstance to open source intelligence.

5.2 OSINT Contributions to Coalition Operations

The *deliberate* establishment of an open source intelligence network within a coalition environment has the following immediate and widespread beneficial effects:

- Assures minimal common appreciation of the situation including terrain and civil factors.
- Enables information-sharing at unclassified level across national and civil-military lines—especially important with non-governmental organizations.
- Significantly enhances information integration and information-sharing within one's own forces.
- Helps to protect sensitive sources & methods.

LtGen Sir John Foley, KCB, OBE, MC, Chief of Defence Intelligence for the United Kingdom, speaking to the “Intelligence in Partnership” conference hosted by the Joint Military Intelligence College in June 1997, noted in his luncheon remarks his concern over the absence of a “common view of the battlefield” in those instances where the allies had more in-depth information and earlier warning from classified systems, while the coalition partners did not.

Establishing the richest possible common view of the battlefield, using open sources, must be a top priority in any coalition operation. Indeed, the distribution of unclassified warning and order of battle information based on classified collection, must become a standard operating procedure.

Even more challenging than the information sharing environment of a military coalition, however mixed, is that of civil-military operations, especially when the civilians are in charge and the non-governmental organizations have learned to distrust the military at the same time that the military has the mistaken belief that it knows everything it needs to know.

Other benefits of open sources within a coalition environment are the enhancement of *internal* coordination, and the ability to protect sensitive sources and methods by passing on the grist without the chaff of secrecy.

5.3 Creating A Joint OSINT Cell and Network

No one who is familiar with the NATO intelligence backbone, EUCES-BICES, would ever want to wish that on their worst of enemies. Although NATO has made progress, the reality is that most coalition partners, and most civilian agencies, will never in this century and most of the next begin to approach the degree of electronic sophistication—one might say the degree of electronic handicapping—that characterizes US/Allied operations.

The fact of the matter is that the quickest easiest way to get things stabilized and establish a modicum of useful information sharing is to create a Joint Open Source Intelligence Cell (JOSIC). Indeed, establishing a JOSIC as part of every military exercise and deployment henceforth is likely to introduce a new standard of compatibility and interoperability impossible to achieve with existing military communications.

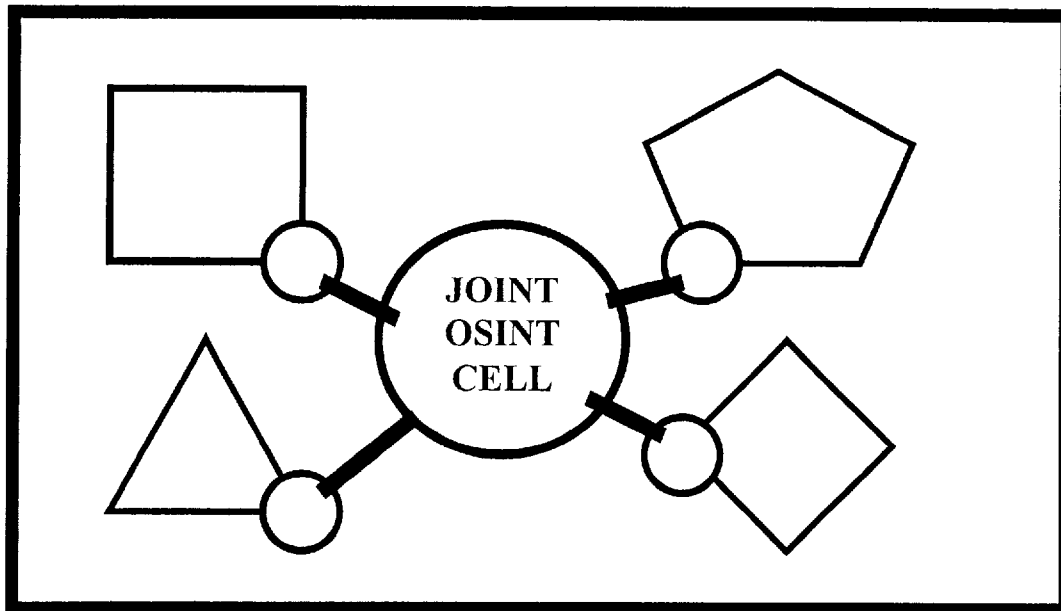


Figure 48: Joint OSINT Cell and Network for Coalition Operations

This new standard must of necessity rely primarily on external communications and computing capabilities that are not controlled by the allied military forces, and that are transparent to non-governmental organizations and others.

Security issues are very important, and the emphasis here on open source intelligence in no way is intended to suggest that security should be lessened, either with respect to classified sources, or with respect to normal operations security (OPSEC).

5.4 OSINT Contribution to Own Force Coordination

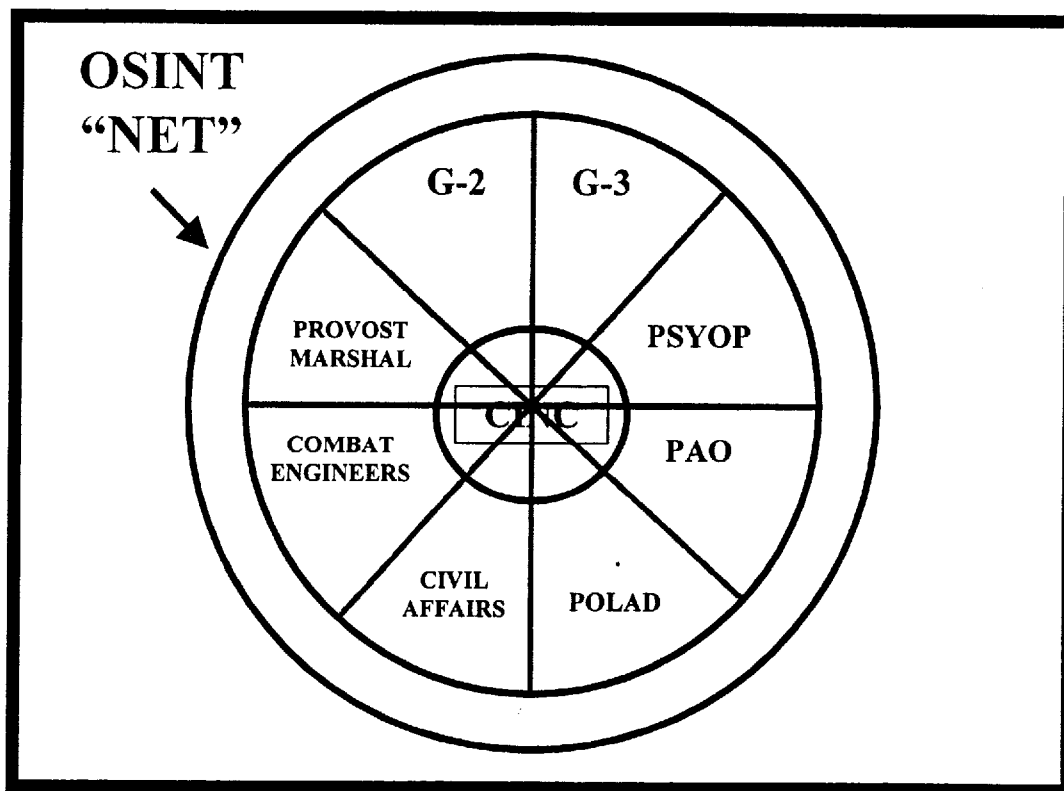


Figure 49: OSINT Contribution to Own Force Coordination

This depiction, borrowed from an excellent article by LtCols Garry J. Beavers and Stephen W. Shanahan,²¹ represents the force multiplier effect within one's *own* forces that can be derived from establishing an open source network.

The Atlantic Command, when it was under General John Sheehan, USMC, was forced, kicking and screaming, to establish an unclassified web site where each of the Colonels in charge of a staff was *required* to post their weekly schedule. Many other items of useful information were posted as well, but the posting of the schedules of the boss Colonels, within weeks, had the remarkable effect of significantly improving staff coordination across sections. Until this initiative by General Sheehan, they had all literally been operating in isolation from one another.

Especially valuable, both in coalition operations and within ones own forces, is the practice of routinely including the PAO, Civil Affairs, the Engineers, the Provost Marshall, and even that irritating civilian “political advisor” in an internal open source intelligence network.

6.0 CREATING A “BARE-BONES” OSINT CELL

6.1 General Purpose. Just what should an OSINT Cell *do*? We thought about this under contract to the Defense Intelligence Agency, and one of the references, available at our web site at no cost (as with all our references) goes into excruciating detail about how one might create a “bare bones” open source intelligence capability.

6.2 Specific Functionalities

- **OSINT Cell Functions Should Include:**
 - **Current awareness briefs/tip-off “bundles”**
 - **Rapid response reference desk**
 - **Primary research**
 - **Strategic forecasting**

Figure 50: Functionality for a “Bare Bones” OSINT Cell

Among the functions of a “bare bones” OSINT Cell should be the provision of current awareness or situation monitoring briefs for each of the key decision-makers and/or their supporting analysts. It should also be able to provide rapid responses to reference questions, contract with outside experts for primary

research, and coordinate strategic forecasting projects drawing on the full range of external open sources, software and services.

OSINT is the starting point for both the intelligence producer and the intelligence consumer, although it should take different forms for each.

However, what we would emphasize is that the vast majority of the OSINT should not be created in-house. If the private sector is to be properly exploited, then most of the OSINT should be done by private sector parties that are able to “mix & match” needed sources, software and services.

6.3 Typical Products. Below is one of our earlier mock-ups of a current awareness product for the all-source analyst.

OSINT CELL-II

MEXICAN INSURGENCY
Wednesday, 3 September 1997

Click for full text →

Mass Media Stories (Commercial Online Services, Edited Content) [EXPAND]

- 01 CHIAPAS INSURGENCY CONTINUES
Associated Press 1500 Words. "The Chiapas Insurgency continues to escalate, with 13 Mexican soldiers
- 02 CHIAPAS LEADERSHIP VISITS GENEVA
Los Angeles Times 1631 Words. "The leaders of the Chiapas insurgencies
- 03 YUKATAN KIDNAPPING OF U.S. BUSINESSMAN
El Tiempo, 764 Words. "Ayer en el sur de Mejico, un empresario Norte Americano fue sequestrado por

Click for full list in section →

Rough translation optional →

Journals (Peer Reviewed Journals, Mostly Off-Line) [EXPAND]

- 01 MOST RELEVANT NEW ARTICLE
"A Comparative Approach To Latin American Revolutions" (Wickham-Crowley, INT J COMP, July 19
- 02 MOST HEAVILY CITED RECENT ARTICLE
"Environmental Scarcity and Violent Conflict: The Case of Chiapas, Mexico" (Howard, Philip and
- 03 MOST RELEVANT NEW FOREIGN LANGUAGE ARTICLE
"Tierra, Pobreza, y Los Indios: La Situacion Revolucionaria en Mejico" (Gonzalez, Juan Fernando,

Abstract may be online; copy can be ordered via email. →

Internet (Caution: Content Not Subject To Editorial Review) [EXPAND]

- 01 NEW SITE MATCHING PROFILE, EZLN
<<http://www.ezln.org>>
- 02 INCREASED ACTIVITY, OVER 1000 HITS YESTERDAY
<<http://www.eco.utexas.edu/faculty/Cleverer/chiapas95.html>>
- 03 New Major Document, "Chiapas—El Pueblo Adelante!" (14 pages)
<<http://www.indians.org/welker/chiapas2.htm>>

Documents can be provided; sites are pointers for client to access.

Number of lines per entry can be changed

Figure 51: Sample Current Awareness Product for All-Source Analyst

We’ve been in production since Feb 1998 and have learned several hard lessons. Among them:

- 1) decision makers and analysts both need an analytical summary. The decision makers want only the summary, the analysts want the summary at the top of the bundle. We now provide that.
- 2) never assume your client, no matter how many billions they are spending on satellites, can handle a simple HTML bundle sent as an email attachment.
- 3) never assume that the product is actually reaching the intended recipient. You have to ask them at the end of each week.
- 4) never assume that you will get feedback. You have to ask for it each week. Eventually the clients will learn that a quick email will pay huge dividends, as when they want to shift the profile to concentrate exclusively on the forthcoming harsh winter needs of war refugees in Bosnia and flooding victims in China.
- 5) never assume your technical people know anything about content. In fact, we went for two months not realizing that half our collection was being “eaten” by our technical people who had improperly programmed the routing thresholds and other bits.

6.4 Staffing Concept. Below is a depiction of what we recommend, and we stress—as strongly as it is possible to stress—that these individuals should not themselves be doing any open source intelligence collection or production.

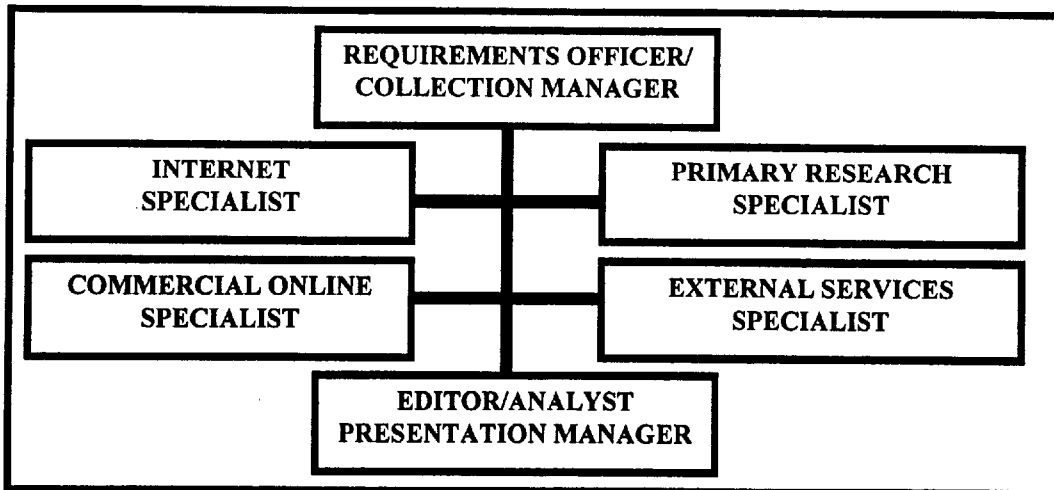


Figure 52: Recommended Staffing for a “Bare Bones” OSINT Cell

The requirements manager is responsible for ensuring that the unit does not accept any “tell me everything about everything” questions, but instead gets specific requirements. This person also manages, in consultation with the respective specialists, the choice of approaches—some requirements will start with the Internet, others will go directly to an expert graduate student or professor.

The others handle their respective areas in terms of farming out the work to private sector support activities, and ensuring quality control as well as cost control.

The Internet specialist uses external specialists, either generalists very skilled at searching the Internet, or subject-matter specialists fully familiar with the Internet, to do “centralized” discovery and either provide the analyst with the full text information, or with bookmarks where the analyst can do exploitation directly.²²

The commercial online specialist orchestrates the creation of profiles and the farming out of the work to the right mix of information brokers or others able to tap into the correct online sources.

The primary research specialist coordinates direct contact surveys and investigations.

Gray literature falls between the commercial online specialist who may use information brokers located in specific countries, or the primary research specialist who may use specialist searchers to obtain materials directly.

The external services specialist focuses on commercial imagery support as well as those offerings listed under services in the Open Source Marketplace™.

The editor/analyst is responsible for ensuring that all incoming and outgoing open source intelligence has the same look and feel and is consistent with organization needs.

6.5 Recommended Approach. Over the past seven years, dealing with representatives from over 40 countries, consulting directly to 18 countries, we’ve formed the strong impression that it is not possible for any single organization or community to “get it right” in a vacuum. The magnitude of the open source opportunity as well as the open source challenge is such that a concerted national effort is required. By this we mean that a national open source intelligence architecture must integrate the needs of the military, law enforcement, business,

and others, and in this way optimize both knowledge about open sources, and prices from vendors.

It is especially important that the various communities: civilian intelligence, military intelligence, law enforcement intelligence, and, outside the government, business intelligence; find a way to establish a central coordination facility while retaining their ability to execute decentralized open source information collection and intelligence production activities.

6.6 Persistent Problems. Problems will persist for at least another ten if not twenty years, with respect to security, funding, and cultural barriers; a training and education vacuum; a concepts and doctrine vacuum; and continuing foreign language deficiencies among both collectors of open source information and producers of open source intelligence.

This is a long term challenge, and the barriers and vacuums will persist for some time. The open source revolution started in 1992. Our calculation is that it will take fully eighteen years—until 2010—before we are possibly satisfied with the state of open source exploitation within intelligence communities *alone*. We expect it to take at least another six years beyond 2010 to extend the concept of the virtual intelligence community to government departments and the larger business community.²³

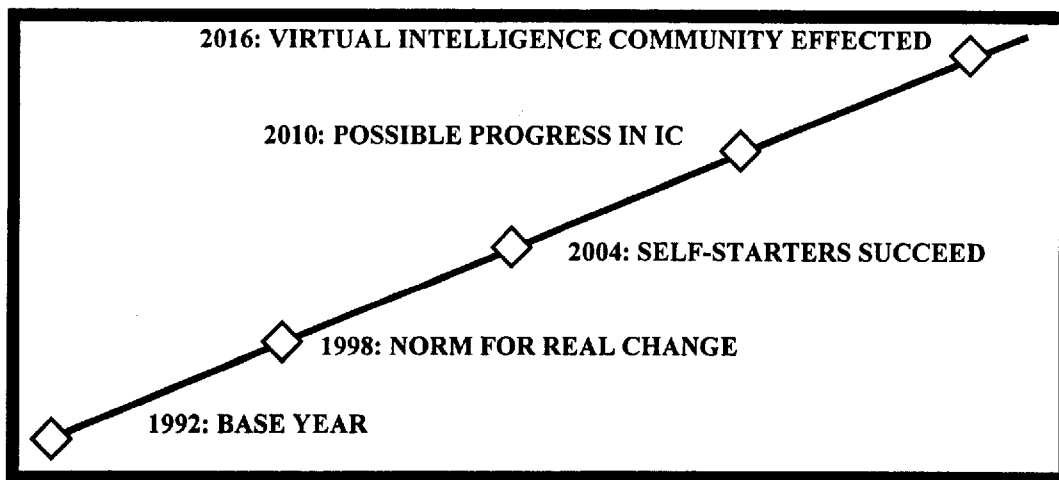


Figure 53: From the Base Year to the Virtual Intelligence Community

6.7 Budgetary Recommendations. We've thought long and hard about how much to spend on open source intelligence, and at the end of the day, based not only on the U.S. Intelligence Community's experience but also on our observations over seven years with eighteen governments, we believe that no less than 1% of the total organizational budget, or in the case of intelligence communities, no less than 5% of their total budget, is required.

A simple way to understand these percentages is in relation to the U.S. defense and intelligence budgets.

- Rough Annual DoD Budget: \$250 billion
- Rough Annual IC Budget: \$25 billion
- 1% of the DoD Budget: \$2.5 billion
- 5% of the IC Budget: \$1.25 billion

Somewhere between \$1.25 billion and \$2.5 billion is the number for the USA. In March 1998 we were invited to draft a Special Report for the Defense Daily Network, and we were pleased to do so. This report included the first ever public itemization of how much the U.S. Department of Defense should spend on open source intelligence, and how this might be allocated. Our numbers are documented in detail within the report, which is listed in the references and available through the Internet.

Commercial imagery acquisition & processing	250M/Yr
Ground stations for receipt of commercial & U.S. national imagery	50M/Yr
Contribution to UN, NATO OSINT cells and network	100M/Yr
Distributed OSINT Cells for CINCS, Services, and Departments	150M/Yr
Training of multiple generations (all ranks)	25M/Yr
Internet seeding to establish useful nodes	25M/Yr
OSINT analysts at embassies with funds to buy local OSINT	50M/Yr
OSINT direct support from private sector	825M/Yr
Contingency or crisis support	25M/Yr
Total Annual Budget	1.5B/Yr

Figure 54: Proposed OSINT Budget for U.S. National Security Purposes

It merits comment that the number for commercial imagery comes from Mr. Doug Smith, Deputy Director of the National Imagery and Mapping Agency, and applies to fulfilling our needs of 1:50,000 with 10 meter imagery. If the much more expensive 1 meter imagery is used, this number doubles.

Such a program would be expected to lead to significant cost savings and significant operational enhancements within the larger \$250 billion a year DoD budget—in essence, for less than 1% of the DoD budget, we believe we can increase the value of the remainder of the DoD budget by at least 10%.

We would also point out that this proposed program would support over 50,000 SI/TK analysts and over 250,000 action officers in the Office of the Secretary, the Services, the theaters, and in major subordinate commands.²⁴

However much one decides to spend, from these calculations we can draw out a generic breakdown of our recommended spending profile.

Commercial imagery acquisition & processing	16%
Ground stations for receipt of commercial & U.S. national imagery	3%
Contribution to regional OSINT cell and network	7%
Distributed OSINT Cells for CINCS, Services, and Departments	10%
Training of multiple generations (all ranks)	2%
Internet seeding to establish useful nodes	2%
OSINT analysts at embassies with funds to buy local OSINT	3%
OSINT direct support from private sector	55%
Contingency or crisis support	2%

Figure 55: Generic Recommendations for National Security OSINT Program

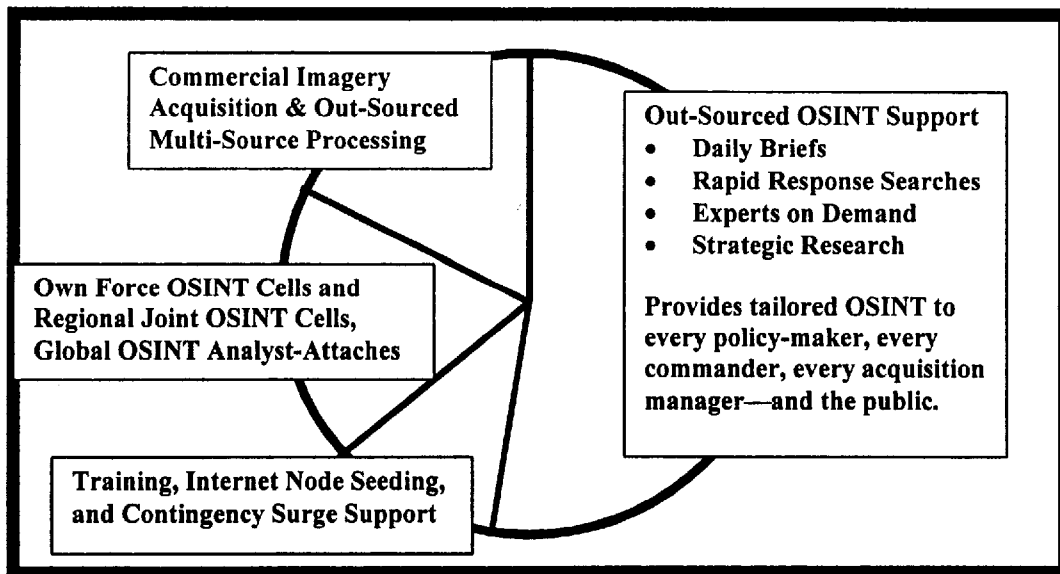


Figure 56: High-Level View of OSINT Spending Categories

7.0 CONCLUSION

7.1 Military Leadership. Here is the bottom line: the military simply cannot do it alone. The open source challenge is too big to just “buy” the solution. It requires a degree of national understanding and cooperation from business and academia that cannot occur through simple contractual relationships. It is also so big that fiscal reality requires that the military pool resources with the policy community in other departments, and with law enforcement, in order to achieve economies of scale in concept and doctrine development, training, procurement, and dissemination.

We do, however, believe that the military in any given nation can and should take the lead. It has been our experience, across the board, that the military tends to be more open-minded than its civilian intelligence counterparts; and that the military is generally blessed with three key ingredients for success in creating a new open source intelligence initiative:

- the discipline and command structure
- the budget flexibility; and
- the best transnational relationships with counterpart forces.

7.2 Information Operations Big Picture. Within the allied military community, and to a lesser extent within selected European and Asian militaries, there has been much discussion of the emerging importance of information warfare and information operations.

The original hyperbole about “information dominance” is now in disrepute. The military has not, however, come to grips with the fact that the bulk of any information operations campaign must be comprised of *content* and ideally of open source intelligence—intelligence coming in to guide the commander and staff; and intelligence going out to influence belligerents, bystanders, and coalition bubbas.

In brief, OSINT turns out to be absolutely essential to the all-source intelligence process; to information warfare operations, and to information peacekeeping operations. OSINT is both an input, and an output. OSINT serves as both a critical foundation for sensitive classified activities, and as an umbrella for orchestrating and nurturing diplomatic activities and military operations other than war. Information Operations is at root an unclassified endeavor that must rely very substantially on discovering, discriminating, distilling, and disseminating open source intelligence.

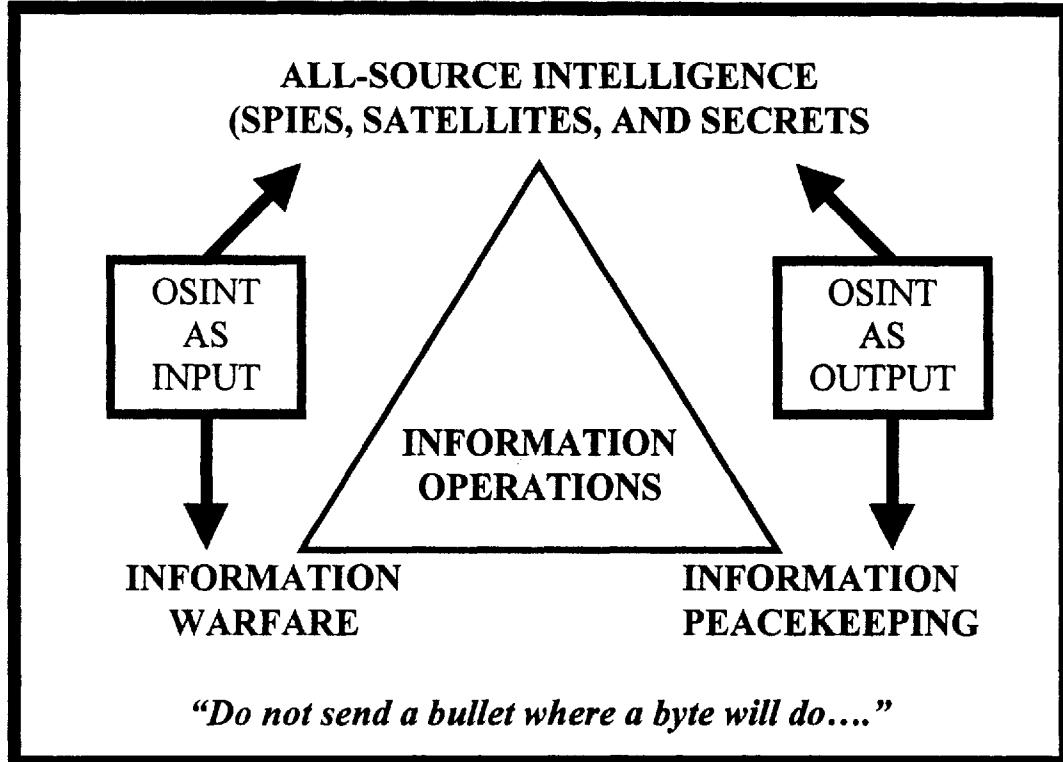


Figure 57: The Information Operations Big Picture

Information peacekeeping and the role of virtual intelligence in avoiding and resolving conflict are discussed in two of the references, both available through the Internet.

We have a long way to go before a byte will be as effective as a bullet. It will take at least a decade—perhaps a half century—before we get desperate enough to actually carry out strategic assessments on vanishing aquifers, the impact of starvation in Africa on Australia, and so on. Only when intelligence steps up to its role as a preventive forecast compelling enough to induce executive action in time of peace, might we be considered skilled at information operations.

7.3 Virtual Global Intelligence Community. The figure below offers a vision of the future in which the intelligence community as we know it becomes a node for harnessing the distributed intelligence of the whole earth. This in turn makes intelligence reform possible, while also enabling a revolution in national security affairs.

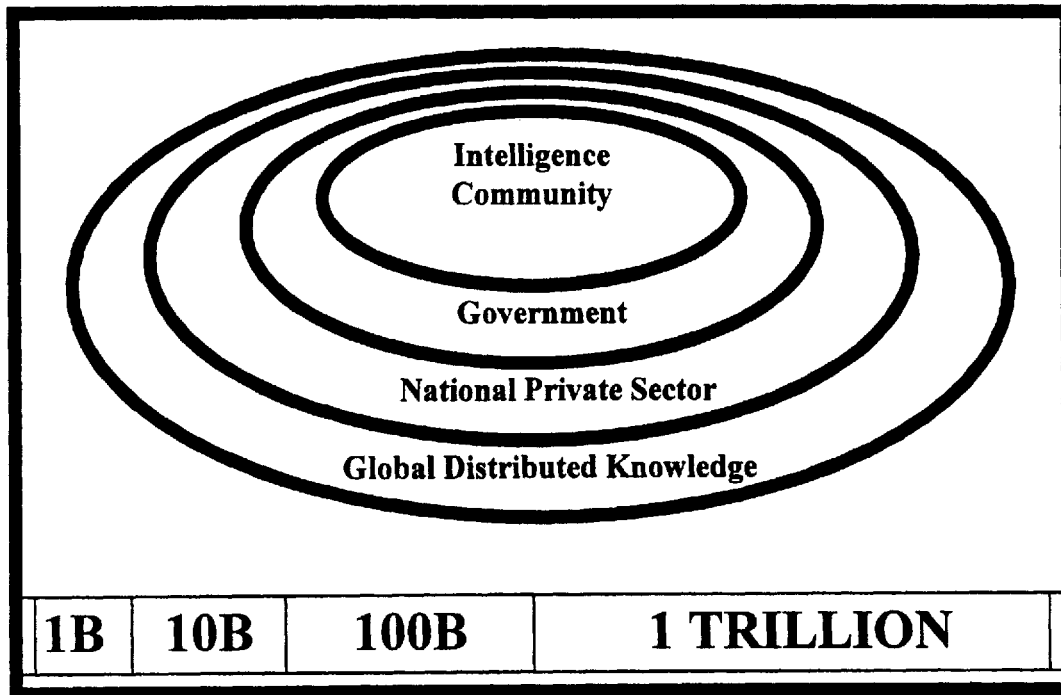


Figure 58: Harnessing the Distributed Intelligence of the Whole Earth

Intelligence communities today spend, in the aggregate, around \$1B a year for open sources. Governments spend around \$10B a year, perhaps even much more. National business communities easily spend \$100B a year. And around the world, overall, our estimate is that a total of at least \$1 trillion a year is spent on those things that we have grouped together as open sources, software and services.

Our objective is grand—it is to transfer the proven methods of national intelligence into the private sector (to include unencumbered encryption necessary to protect intellectual property and facilitate remote exchanges), while at the same time creating an architecture, a network, through which every citizen and every organization can be “smart” and have access to open source intelligence.

This is what we call the “virtual intelligence community.”

7.4 Intelligence Reform: Striking a New Balance. The U.S. Intelligence Community has probably been the most studied in history. Over time, the constant refrain has been about excess. Excessive spending on technology. Excessive emphasis on collection to the detriment of analysis. Excessive secrecy.

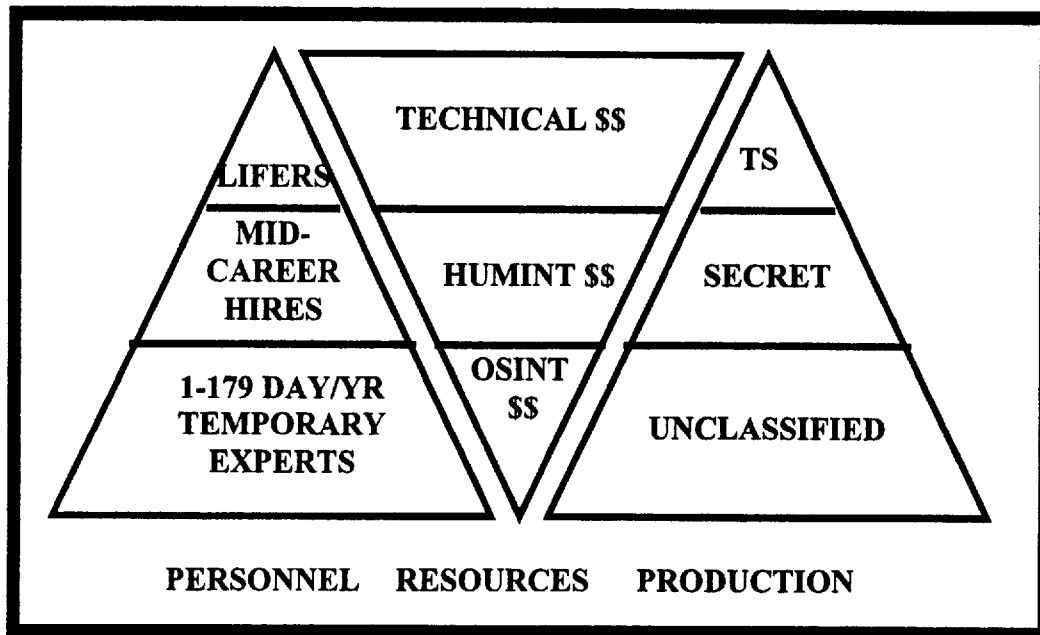


Figure 59: Striking A New Balance

In the future, and in the context afforded by the emerging appreciation of open sources and the potential of an international “virtual intelligence community”, it is our view that very significant changes will be required, resisted, and then valued.

People will come to the intelligence community at mid-career, after proving themselves in an international private sector specialty. Most people will not become permanent employees, but rather serve as required. Resources will be moderately shifted from technical collection to human analysis and open source procurement. Secrecy will take a back seat to unclassified intelligence production that can be shared across organizational, national, and even cultural boundaries.

Put another way, the classic spy will give way to the modern spy. There will be a shift in emphasis from collection to analysis; from technical intelligence to human intelligence; from technology applied to collection to technology applied to processing what we already have; from creating Codeword products for an elite to creating open source For Official Use Only (FOUO) or RESTRICTED products that we can share.

At the end of the day, the government will be able to get 100 to 500 times as much “intelligence” value without changing its existing budget, and—if we are

able to transfer methods to the business and law enforcement communities—we will see a day when their expenditures for intelligence match those of the national governments, and we have an international “virtual intelligence community” of staggering utility.

7.5 Revolution in National Security Affairs. The classic spy is not capable of dealing with all four of the warrior classes or forms of war that will challenge us in the 21st Century. We will still need the classic spy, and clandestine technical collection capabilities, but they will have to be carefully focused across all four of the threat classes, and they will have to be focused in a manner that is only possible if we are able to master open source intelligence.

“Net assessment” is not yet well defined or well practiced because it does not appreciate the four levels of analysis, it does not focus on three of the four warrior classes, and it does not do strategic comparisons between private sector capabilities in the home country versus those of other countries. “Net assessment” in the future will require far more subtlety, to include cultural, demographic, and health assessments, and it will have to be focused on radically impacting on *domestic* policy decisions in the *global* context.

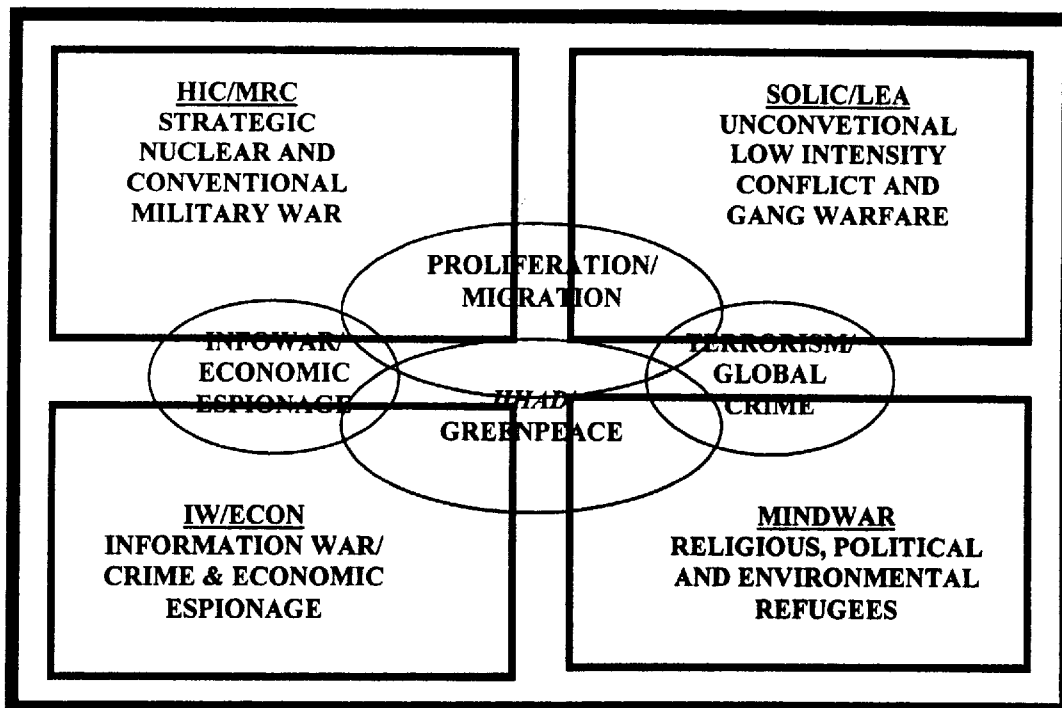


Figure 60: Four Threats, Four Defense Forms

7.6 National Information Strategy. Military success in exploiting open sources, and the creation of a “virtual intelligence community” able to meet the intelligence needs of all citizens and organizations, will only be possible within those nations that deliberately choose to craft and implement a *national information strategy*.

We proposed such a strategy for the United States of America in 1994, without effect. The strategy addressed four elements:

- 1) Connectivity, to include free Internet access and more robust infrastructure to carry the bandwidth explosion;
- 2) Content access and validation nodes, in effect creating a distributed open source intelligence community in which specific organizations assume responsibility for first echelon collection and processing for their assigned area of interest;
- 3) Coordination of both standards and investments, without which no nation can afford to abandon its aging industrial information architecture and adopt a modern information architecture; and
- 4) C4 security, absolutely vital to the survivability and credibility of the whole.

OSINT, at root, is about creating a “smart nation.”

At this strategic level of thinking, the U.S. military in particular (both at the policy level and at the uniformed command level) is especially handicapped. The information revolution has dramatically altered the fundamental nature of the relationship between military and civilian organizations; between government and the private sector; between weapons systems and targeting information; between “battlefield awareness” and “public perception”.

The military cannot survive in this environment if it persists in its obsessive belief that it must control all communications and computers associated with its missions, and if it persists in believing that it is the only party to an operation other than war that can be relied upon to orchestrate information operations.²⁵

The military has much to offer, including leadership, as we move toward national information strategies, but until the military learns to give up “control” in order to achieve “coordination” across relevant sectors, it will be its own worst enemy.

7.7 **OSINT Building Blocks.** If one has a national information strategy, or a commitment among various communities to attempt to establish a national information strategy with the four elements listed above, then it becomes possible to bring together various OSINT building blocks.

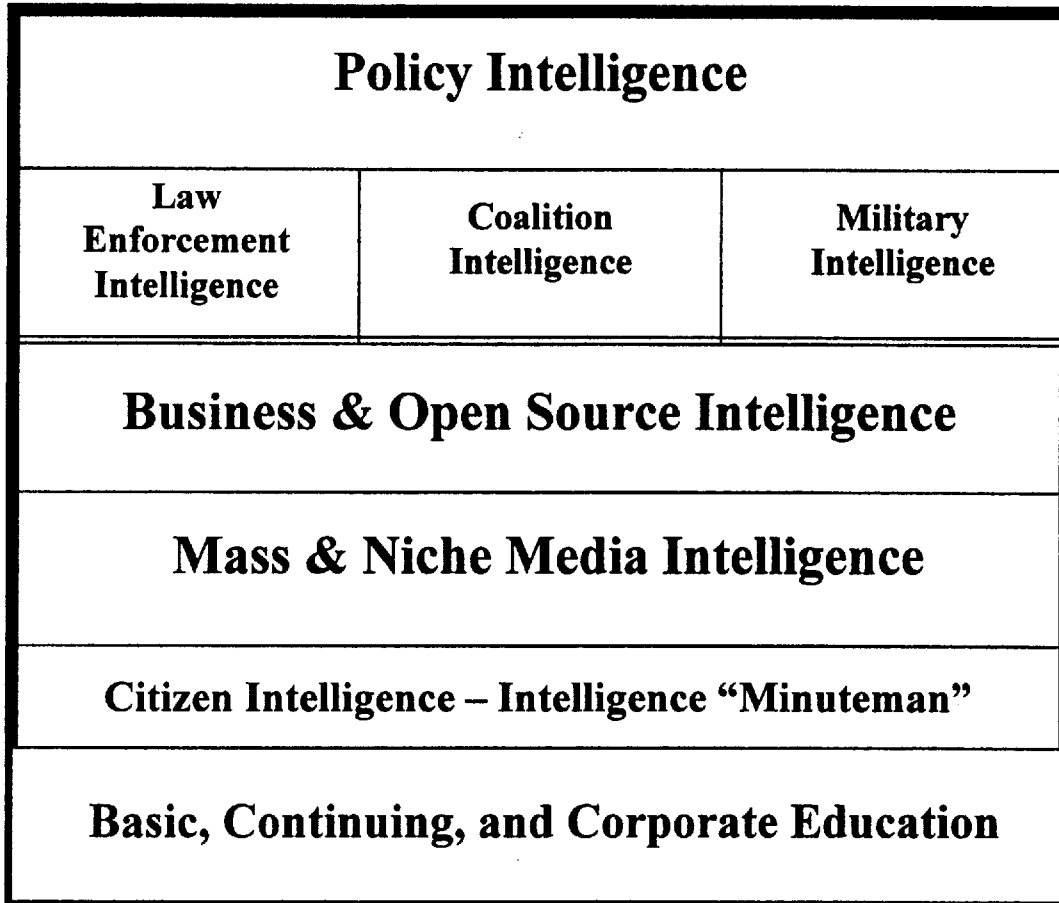


Figure 61: OSINT Building Blocks²⁶

No one has a “national” intelligence community today. Most countries have a military and a civilian intelligence organizations--or several organizations that quietly ignore one another. No country really has an effective law enforcement intelligence community, or business intelligence community. In most countries the media runs the gamut from sensationalist to pedestrian. Citizens do not understand nor apply the methods of intelligence, and education is generally abysmal. It is possible, however, to sensitize these various communities to the possibilities, using the following illustration.

This is our challenge. We need to elevate each of these blocks to “best in class” status, and we need to break down the barriers between each of these communities so that they are able to share basic open source information.

7.8 Information-Driven Government Operations. If we are even moderately successful at understanding both the value of information and the degree to which we are at risk while failing to modify our approach to information, then we may eventually understand that we need a government that is driven by information. It must be a government in which capabilities correspond to both threat classes, and to the utility of information in the accomplishment of specific kinds of missions.

This is what it might look like:

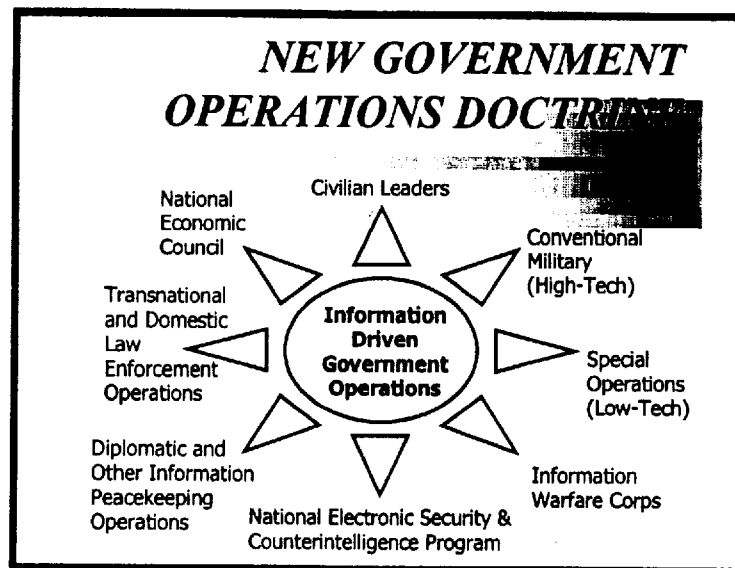


Figure 62: Information-Driven Government Operations for the 21st Century

That is the open source story. It is a revolution, not only in concepts and doctrine as they apply to national and military intelligence, but also as they apply to government operations and the very fabric of the national spirit. Open source intelligence is, at root, about creating a “Smart Nation” in which every citizen is an “intelligence minuteman”—every citizen is a collector, producer, and consumer of open source intelligence.

*A Nation’s best defense is an educated citizenry.*²⁷

8.0 NOTES

8.1 References

- Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations" (Defense Daily Network, 4 March 1998) at www.defensedaily.com/reports/osint.htm
- *Open Source Intelligence: HANDBOOK* (Joint Military Intelligence Training Center, October 1996) at www.oss.net/HANDBOOK
- *Open Source Intelligence: READER* (OSS Inc., 1997) at www.oss.net/READER
- *Concept Paper: Creating a Bare Bones Capability for Open Source Support to Defense Intelligence Analysts* (OSS Inc., 18 August 1997) at www.oss.net/DIAReport
- "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community" (Major Robert M. Simmons, Joint Military Intelligence College, August 1995)
- "Virtual Intelligence: Conflict Avoidance and Resolution Through Information Peacekeeping", *Proceedings of the Virtual Diplomacy Conference of 1-2 April 1997 in Washington, D.C.* (U.S. Institute of Peace) at <http://www.oss.net/VIRTUAL>
- *Intelligence and Counterintelligence: Proposed Program for the 21st Century* (OSS Inc., 14 April 1997) at <http://www.oss.net/OSS21>
- "Information Peacekeeping: The Purest Form of War" in *CYBERWAR: Myths, Mysteries, and Realities* (AFCEA, 1998) at www.oss.net/InfoPeace
- Other references including self-study OSINT lessons at www.oss.net

8.2 Training

- **Open Sources (Online, Offline), Software Tools, and Niche Services**
- **Oriented Toward the All-Source Government Intelligence Professional**
- **Cross-Fertilization with Law Enforcement and Business Intelligence**
- **All Events include Networking Breakfasts, Luncheons, and Receptions**



PacInfo '98 **7-9 Dec 98** **Monterey, CA**
 Pacific Information Forum including OSINT Operations Pre-Conference Course.
 In association with Monterey Institute of International Studies, other organizations.
 Emphasis on non-governmental organizations, information-sharing methods.



EuroIntel '99 **9-11 Mar 99** **The Hague**
 European Intelligence Forum including OSINT Operations Pre-Conference Course.
 In association with EUROPOL and the Association for Global Strategic Information.
 Emphasis on transnational criminal, terrorist, and proliferation targets.



OSS '99 **24-26 May 99** **Washington, D.C.**
 Global Intelligence Forum including OSINT Operations Pre-Conference Course.
 Includes affiliated conferences sponsored by professional intelligence associations.
 Includes electronic job fair for both government and industry intelligence positions.

OSS Inc. offers both national-level seminars tailored to the needs of specific communities in their home countries, and individualized training at the OSS Inc. facilities in Fair Oaks, Virginia. OSS Inc. manages a global Rolodex of open source intelligence professionals available as speakers, teachers, consultants, and expert collectors or producers.

8.3 Endnotes

¹ Dr. Joseph Markowitz, Director of the Community Open Source Program Office (COSPO) within the Office of the Director of Central Intelligence (USA), is the originator of this important distinction between OSINT as practiced in the private sector, and OSINT as potentially beneficial to national intelligence communities. At one stroke he eliminated concerns that OSINT might displace all-source analysis.

² Dr. Lowenthal devised this new concept to demonstrate the urgency of developing an open source intelligence process to address the growing gap between what intelligence agencies could know versus what they can use.

³ This figure presents a hard, candid, and ultimately fair evaluation of how we do against each of the four warrior classes. A more detailed study of our deficiencies, both against each of these threat classes and in relation to the levels of analysis (next slide) is provided in "A Critical Evaluation of U.S. National Intelligence Capabilities", *International Journal of Intelligence and Counterintelligence* (Summer 1993). Explicit proposals for improving our national intelligence and counterintelligence capabilities to deal effectively with all four challenges are also provided in *Intelligence and Counterintelligence: Proposed Program for the 21st Century* (OSS Inc., 14 April 1997) at <http://www.oss.net/OSS21>.

⁴ AFP world news summary for Friday August 21 (since 0930 GMT) Agence France-Presse, 08/21/1998, 483 words. US-bombs-toll ISLAMABAD: US missile strikes on alleged terrorist targets in eastern Afghanistan killed 26 people and injured around 40.

⁵ DCI: Director of Central Intelligence; D/CSIS: Director, Canadian Security and Intelligence Service; D/NPC: Director, Non-Proliferation Center; D/COSPO: Director, Community Open Source Program Office.

⁶ "In some areas, such as economic analysis, it is estimated that as much as 95% of the information utilized now comes from open sources...an adequate infrastructure to tie intelligence analysts into open source information does not appear to exist...[this] should be a top priority for the DCI and a top priority for funding." *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Report of the Commission on the Roles and Capabilities of the United States Intelligence Community, 1 March 1996), page 88.

⁷ The report of the Commission on Protecting and Reducing Government Secrecy, under the leadership of Senator Daniel Patrick Moynihan (D-NY), was released on 4 March 1997. Mr. Steele testified to this Commission several times, including once in a personal session with Senator Moynihan at the Senator's request. Mr. Steele's extensive written comments on the costs of secrecy are available in "TESTIMONY to the President's Inter-Agency Commission on National Security Information", Department of Justice, 9 June 1993.

⁸ In Thomas P. Coakley (ed.), *C3I: Issues of Command and Control* (National Defense University, 1991), page 68.

⁹ The Commission on Secrecy that reported out in the United States of America in 1997 was not quite so dramatic, but they did note that we spend \$6 billion or more a year protecting classified information already collected, and they did raise the interesting concept of "transaction costs"--a

concept that might ultimately lead to OSINT versus all-source “jousts” to see if OSINT is “good enough”, for thousands of dollars, when compared with “perfect” all-source production requiring hundreds of thousands of dollars in collection and processing and analysis costs.

¹⁰ The rapid planning process and the unplanned nature of most contingencies generally requires staff to scramble for their encyclopedic and orientation intelligence. The *Expeditionary Factors Study*, the flagship publication of the U.S. Marine Corps Intelligence Center, is a good example of an “off-the-shelf” product that uses only open sources to provide distilled operational intelligence about 80 countries, across roughly 143 mission area factors. It is available on both the Open Source Information System (OSIS) and INTELINK-C. MCIA Point of Contact for access to this FOUO/RESTRICTED product is Ms. Dana Harman at (703) 784-6144.

¹¹ This compilation of specific capabilities and specific companies is not always appreciated, but offers insights into just how varied the sources, software, and services offerings can be.

SOURCES	SOFTWARE	SERVICES
Current Awareness (e.g. Individual Inc.)	Internet Tools (e.g. NetOwl, Copernicus)	Online Search & Retrieval (e.g. NERAC, Burwell Directory)
Current Contents (e.g. ISI CC Online)	Data Entry Tools (e.g. Vista, BBN, SRA)	Media Monitoring (e.g. FBIS via NTIS, BBC)
Directories of Experts (e.g. Gale Research)	Data Retrieval Tools (e.g. RetrievalWare, Calspan)	Document Retrieval (e.g. ISI Genuine Document)
Conference Proceedings (e.g. British Library, CISTI)	Automated Abstracting (e.g. NetOwl, DR-LINK)	Human Abstracting (e.g. NFAIS Members)
Commercial Online Sources (e.g. LN, DIALOG, STN)	Automated Translation (e.g. SYSTRAN, NTIS-JV)	Telephone Surveys (e.g. Risa Sacks Associates)
Risk Assessment Reports (e.g. Forecast, Political Risk)	Data Mining & Visualization (e.g. i2, MEMEX)	Private Investigations (e.g. Cognos, Pinkertons, Parvus)
Maps & Figures (e.g. East View Publications)	Desktop Publishing & Communications Tools	Market Research (e.g. SIS, Fuld, Kirk Tyson)
Commercial Imagery (e.g. SPOT, Autometric)	Electronic Security Tools (e.g. SSI, PGP, IBM Cryptolopes)	Strategic Forecasting (e.g. Oxford Analytica)

¹² This specific image is a notional construction used by the Soviets in their training materials. While it is labeled as Charkov, Russia, located at E65 long and N49 lat, we checked and it isn't.

¹³ It has been suggested to the National Imagery and Mapping Agency (NIMA) that they should rapidly procure this entire stock, available at a fraction of the cost of duplicating it. In combination with precision data from U.S. national satellites, and commercial imagery, this would create a global geospatial database superior to anything heretofore possible or likely to be possible for decades to come.

¹⁴ Colonel James “Snake” Clark is the program manager within the office of the Vice Chief of Staff of the Air Force. He can be reached at voice: (703) 693-3377, facsimile: (703) 693-0155, or email to jlclark@msis.dmsomil.

¹⁵ SPOT Image, a French company, has the world's only industrial strength commercial imagery system, with multiple satellites, two day revisitation times to achieve synoptic imagery necessary to create contour lines, seventeen ground stations world-wide, and--this is incredibly important: *most of the world already in their archives, less than three years old, and cloud-free*. They had all of Burundi, less than three years old, and cloud-free.

¹⁶ Although very heavily used by the U.S. Air Force for general attack missions during the Gulf War, 10 meter commercial imagery is not good enough for precision targeting, CE90 or 3m or less).

¹⁷ The best examination of open source exploitation within defense intelligence that is known to exist is a post-graduate intelligence program thesis, "Open Source Intelligence: An Examination of Its Exploitation in the Defense Intelligence Community" (Major Robert M. Simmons, Joint Military Intelligence College, August 1995). Included in the these was an examination of how open source, more often than not, is the tip-off on new weapons systems and sales.

¹⁸ The best statement of this concept remains that of Mr. Andrew Shepard, "Intelligence Analysis in the Year 2002: A Concept of Operation", presented first at the Symposium on Advanced Information Processing and Analysis (24-26 March 1992) and then in December to the first annual international conference on open source intelligence, OSS '92 and available still in *Open Source Intelligence: READER*.

¹⁹ These and the other strategic generalizations were drawn from *Overview of Planning and Programming Factors for Expeditionary Operations in the Third World* (Marine Corps Combat Development Commands, March 1991), for which the author served as Study Director.

²⁰ Mr. Hugh Smith is on staff at the Australian Defence Studies Centre within the Australian Defence Force Academy.

²¹ "Operationalizing IO in Bosnia-Herzegovina" (in *CYBERWAR: Myths, Mysteries, and Realities* (AFCEA, 1998). See also in the same book, Larry K. Wentz, "Coalition Information Operations: The IFOR Experience".

²² The national intelligence service of The Netherlands appears to do this well, and calls the process one of "centralized discovery, decentralized exploitation". The key thing to remember with this and all other sources is that search skills are distinct from analysis skills, and the purpose of the OSINT Cell is to facilitate discovery by skilled searchers working in their respective mediums, thus enabling the analyst to focus on their core competency, analysis.

²³ The political science literature suggests that it takes six years to implement substantial change when an organization is under effective leadership. We speculate that within bureaucracies the time is doubled, and within bureaucracies bound by secrecy, it is tripled. Hence, from 1992 to 2010 is our realistic estimate of how long it will take the U.S. Intelligence Community to heal itself and adjust to the realities of today's information environment.

²⁴ Specifics include 10 JOINT VISIONS per year at \$5M each; 15 OSINT Cells per year at \$10M each inclusive of personnel costs; 100 analysts at Embassies around the world, each with \$500K a year to spend on procurement of local knowledge; a direct support program that would include

10,000 strategic forecasts at \$25K each (e.g. for critical technologies and all of the acquisition project managers), 25,000 experts on demand at \$6,000 each, 300,000 extended search queries at \$1000 each, and 50,000 integrated current awareness profiles at \$2,500 each; and finally, for contingency surge support, 10 are assumed at \$250,000 each.

²⁵ The sudden and obsessive move by the Pentagon to strip all of its web sites, most of them created through local initiative, of any information that might be conceivably useful to “the enemy” has probably set the U.S. military back at least five years. In an open environment, it is vastly more important to be open and aware in an aggressive manner, than to be closed off and “unaware” in a defensive manner. The Pentagon’s September 1998 retreat from the Internet is the cyberspace equivalent of adopting a Maginot Line posture.

²⁶ The concept of the “intelligence minuteman” was devised by Alessandro Politi from Italy, over dinner at OSS '92. Independently Anthony Fedanzo has contributed “Implementing Open Source Intelligence Through a Distributed Contribution Model”, in *Open Source Intelligence: READER*.

²⁷ A wiser man than either author said this, but we were unable to find a direct attribution in readily available references.

PacIntel '99 PRE-CONFERENCE OPEN SOURCE INTELLIGENCE BASIC TRAINING

- Link Page

[Previous](#) [Ref: Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations](#)

[Next](#) [Ref: Creating a 'Bare Bones' Capability for Open Source Support to Defense Intelligence Analysts](#)

[Return to Electronic Index Page](#)