10

Open source intelligence

Robert David Steele

Executive summary[1]

Definition and scope

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

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

Open source intelligence and joint or coalition operations

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

Private sector information offerings

The Internet is now the default Command and Control, Communications, Computing, and Intelligence (C4I) architecture for virtually the entire world. The principal exceptions are

Robert David Steele, "Open Source Intelligence," in Loch Johnson (ed.), *Handbook of Intelligence Studies* (NY: Routledge, 2007), Chapter 10 pp. 129-147 most militaries and intelligence organizations. The Internet facilitates commerce, provides entertainment and supports ever increasing amounts of human interaction. To exclude the information flow carried by the Internet is to exclude the greatest emerging data source available. While the Internet is a source of much knowledge, all information gleaned from it must be assessed for its source, bias and reliability.

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

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

The open source intelligence cycle

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

OSINT and the emerging future intelligence architecture of NATO

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

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

While unable to replace classified intelligence production, OSINT is able to complement an all-source intelligence production process with essential support including tip-offs, context, validation and cover for information sanitation.[2]

Introduction to open source intelligence

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

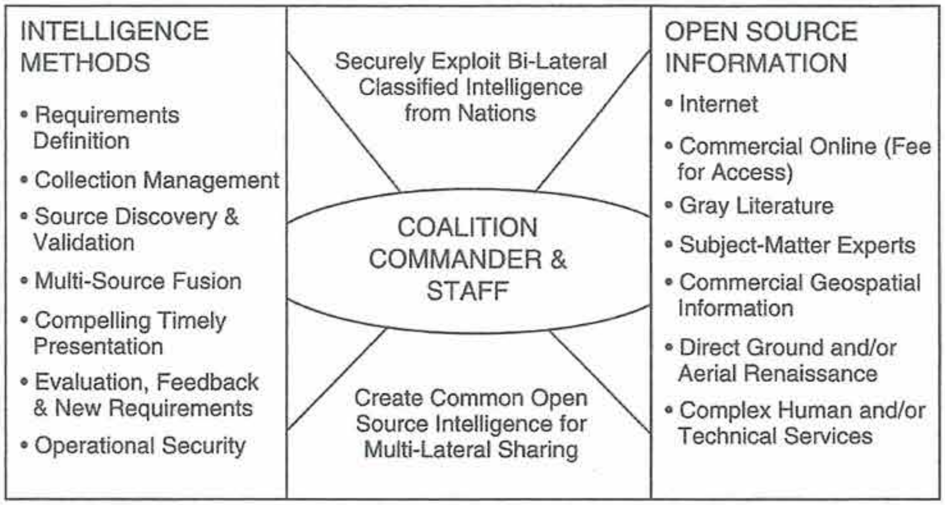

INTELLIGENCE METHODS
• Requirements Definition
• Collection Management
• Source Discovery & Validation
• Multi-Source Fusion
• Compelling Timely Presentation
• Evaluation, Feedback & New Requirements
• Operational Security
Securely Exploit Bi-Lateral Classified Intelligence from Nations
COALITION COMMANDER & STAFF
Create Common Open Source Intelligence for Multi-Lateral Sharing
OPEN SOURCE INFORMATION
• Internet
• Commercial Online (Fee for Access)
• Gray Literature
• Subject-Matter Experts
• Commercial Geospatial Information
• Direct Ground and/or Aerial Renaissance
• Complex Human and/or Technical Services

Figure 10.1 Relationship between open and classified information operations

OSINT is distinct from academic, business, or journalistic research in that it represents the application of the proven process of national intelligence to the diversity of sources, with the intent of producing *tailored* intelligence for the commander. OSINT is also unique, within a coalition operations context, in that it simultaneously provides a multi-lateral foundation for establishing a common view of the shared Area of Operations (AOR), while also providing a context within which a wide variety of bi-lateral classified intelligence sharing arrangements can be exploited. Figure 10.1 illustrates these relationships.

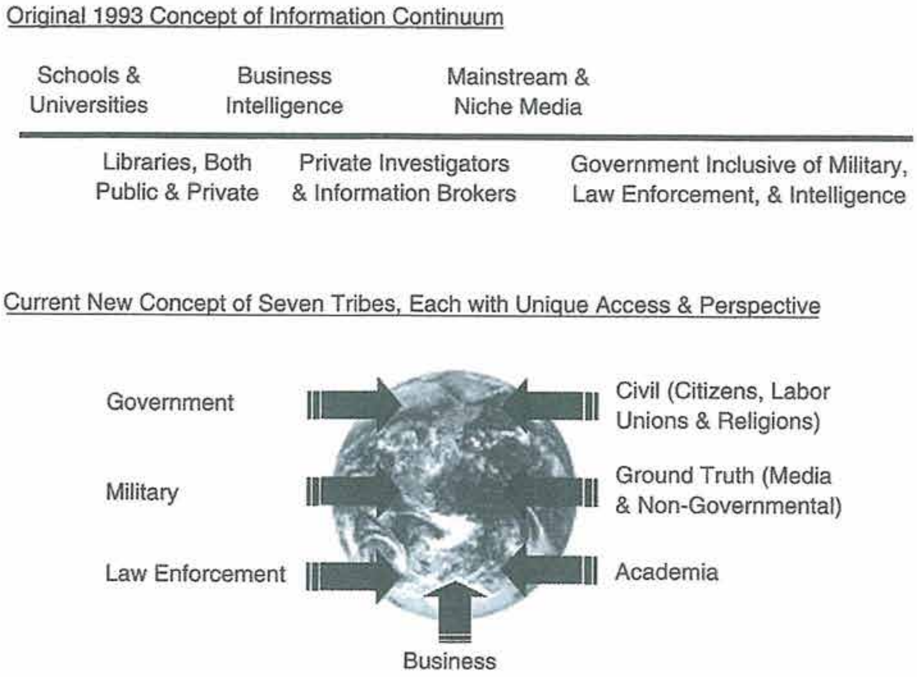
Since 2001, the Swedish government has advanced a concept for Multinational, Multi-agency, Multidisciplinary, Multidomain Information Sharing (M4IS), and the author has put forward the need for regional Multinational Information Operations Centers (MIOC). At the same time, in the private sector, organizations such as the Co-Intelligence Institute have brought forward robust concepts for Collective Intelligence, and books have been written about *Smart Mobs* and *Wisdom of the Crowds*. It is clear from these developments that OSINT is taking on a life of its own outside the government, in keeping with the author's original depiction of the seven tribes of intelligence (see Figure 10.2).[3]

OSINT is less about specific sources such as are listed in the column on the right of Figure 10.1, and more about "knowing who knows."[4]

Definitions

There are four distinct categories of open information and intelligence.

- *Open Source Data (OSD).* Data is the raw print, broadcast, oral debriefing or other form of information from a primary source. It can be a photograph, a tape recording, a commercial satellite image, or a personal letter from an individual.
- *Open Source Information (OSIF).* OSIF is comprised of data that can be put together, generally by an editorial process that provides some filtering and validation as well as presentation management. OSIF is generic information that is usually widely disseminated. Newspapers, books, broadcast, and general daily reports are part of the OSIF world.


Original 1993 Concept of Information Continuum

Schools & Universities
Business Intelligence
Mainstream & Niche Media
Libraries, Both Public & Private
Private Investigators & Information Brokers
Government Inclusive of Military, Law Enforcement, & Intelligence

Current New Concept of Seven Tribes, Each with Unique Access & Perspective

Government
Military
Law Enforcement
Civil (Citizens, Labor Unions & Religions)
Ground Truth (Media & Non-Governmental)
Academia
Business

Figure 10.2 Information continuum and the Seven Tribes

- *Open Source Intelligence (OSINT).* OSINT is information that has been deliberately discovered, discriminated, distilled, and disseminated to a select audience, generally the commander and their immediate staff, in order to address a specific question. OSINT, in other words, applies the proven process of intelligence to the broad diversity of open sources of information, and creates intelligence.
- *Validated OSINT (OSINT-V).* OSINT-V[5] is OSINT to which a very high degree of certainty can be attributed. It can be produced by an all-source intelligence professional, with access to classified intelligence sources, whether working for a nation or for a coalition staff. It can also come from an assured open source to which no question can be raised concerning its validity (images of an aircraft arriving at an airport that are broadcast over the media).

OSINT in context

In this summary chapter we will touch lightly on the context of OSINT, while distinguishing between OSINT as it supports government Intelligence & Information Operations (I2O) where secret sources and methods play a paramount role, and OSINT as the sole legal means of decision support for non-governmental organizations.

While OSINT is not "new" in that nations and organizations have always understood the value of legal travelers, direct observation, structured reading, and legal purchases of information services, what is new about OSINT is the confluence of three distinct trends: first, the proliferation of the Internet as a tool for disseminating and sharing overt information in all languages; second, the consequent and related "information explosion" in which published useful knowledge is growing exponentially; and third, the collapse of formerly denied areas accompanied by the explosion of non-traditional threats in the form of failed states and transnational non-state threats to public security and prosperity.

Below are four perspectives of how OSINT relates to the secret intelligence world, to the specific secret disciplines, to the wisdom of the crowds, and to the decision support process of any commander or Chief Executive Officer (CEO).

1 Open source information (OSIF) is the earth beneath the temple, while OSINT is the foundation, with each of the secret disciplines being a pillar, all holding up the temple's roof, all-source analysis. However, in recent years it has grown in importance, to the point that Dr John Gannon, former Deputy Director of Central Intelligence for Analysis & Production (ADDCI/A&P) is now on record as saying "Open-source information now dominates the universe of the intelligence analyst, a fact that is unlikely to change in the foreseeable future."[6]
2 If intelligence were a baseball game, then the clandestine service would try to recruit a player, the signals intelligence specialists would put a "bug" in the opposing team's dug-out, the imagery people would take a satellite picture of the game every three days. OSINT tells everyone in the audience that if they catch the ball, we will pay cash and it is an out. OSINT changes the rules of the game.
3 OSINT is both a subordinate discipline to each of the classified disciplines, and also uniquely an all-source discipline that can "stand alone" when necessary, combining overt humans, overt signals, commercial imagery, and public analysis.
4 OSINT is the only discipline that can simultaneously access all that can be known in all languages back in time, harness all available expertise and manpower without clearances, and produce intelligence that can be shared with anyone. This makes it especially valuable for law enforcement investigations, humanitarian assistance missions, and early warning for open discussion among members of the United Nations.[7]

OSINT and information operations

Information Operations (IO) is comprised of Information Peacekeeping (IP) and Information Warfare (IW). At the strategic level, IO is broadly related to influencing and messaging all parties (hostile, neutral, and friendly) for national advantage. IO must integrate OSINT (understanding their reality as well as our own), Joint Information Operations Centers or Commands (JIOC) as well as multinational and national variants (MIOC, NIOC) which comprise the tool-sets as well as the mind-sets; and Strategic Communication (the message).

At the operational and tactical levels, this translates into assuring one's own ability to see, hear, know, understand, decide, and act on "all information, all languages, all the time," while denying or distorting or altering adversarial information capabilities.[8]

This is an extraordinarily complex undertaking that has not been intellectually defined. The concepts, doctrines, tools, and mind-sets are a long way from being robust. What this means in practice is that nations and organizations must be able to devise unified campaign plans that fully integrate, on an interagency or inter-departmental basis, the activities of public diplomacy and public affairs or relations, strategic communication and influence (as well as strategic acquisition and force structure management), perception management, psychological operations (PSYOP), the propaganda and agent of influence aspects of covert operations (among governments), denial and deception, space control, network attack and defense, electronic warfare, information and communications and electronic security operations, information assurance operations, counter-intelligence and counter-deception operations, and so on.[9] Rarely emphasized except by the author, all of these demand that we understand reality, and not allow the United States to be driven into bankruptcy by ideological fantasies and consequent policy-level misjudgments.

OSINT and national security

It is a common misperception that most "intelligence" is classified and must come from secret sources and methods that are very expensive and relatively risky. The "cult of secrecy" has put us in a very disadvantageous position, where in the United States of America (USA) at least $50 billion a year is spent on collecting the 5 percent of the information that is secret and can or must be stolen, and virtually nothing is spent on the 95 percent of the information in all languages that is relevant to all but the most secretive threats.

The importance of this observation can be emphasized by listing the top threats to global security as documented in the Report of the High-level Panel on Threats, Challenges and Change, *A More Secure World: Our Shared Responsibility*:[10]

• **Economic and social threats including**	**95%**
– poverty	99%
– infectious disease and	95%
– environmental degradation	90%
• **Inter-state conflict**	**75%**
• **Internal conflict, including**	**90%**
– civil war,	80%
– genocide and	95%
– other large-scale atrocities	95%
• **Nuclear, radiological, chemical, and biological weapons**	**75%**
• **Terrorism**	**80%**
• **Transnational organized crime**	**80%**

Figure 10.3 OSINT relevance to global security threats

The average utility and relevant of OSINT to these global threats is – on the basis of my informed estimate – 82.5 percent, which comes very close to the generic "80–20" rule. We must conclude that any nation that persists in spending 99.9 percent of its intelligence funds on collecting secrets,[11] and less than one half of one percent of its intelligence funds on OSINT, is quite literally, clinically insane (or insanely corrupt) at the highest levels.

Naturally there are those who will quibble about whether the budgets of the National Aeronautics and Space Agency (NASA) or the Environmental Protection Agency (EPA) or the Department of Justice (DoJ) should be "counted." What matters here is that intelligence is nothing more or less than decision-support for the President and the top members of the Cabinet, as well as Congress in its oversight role. Most of the US Government budget, by way of example, is spent on weapons, manpower, and administration. Research & development (R&D) is focused on investigation, design, and the creation of capabilities, not on decision-support. Intelligence is *decision-support.*

It merits comment that those business enterprises and religions that choose to emphasize industrial espionage or the covert subversion of governments are making the same fundamental error of confusing "secret sources and methods" with "intelligence." Intelligence is information that has been collected, processed, analyzed, and presented in order to support a decision that increases security or profit, or reduces risk or cost. Nowhere is it written that "intelligence" must be secret or that intelligence is improved by a reliance on secret sources or methods.

Indeed, it has been demonstrated on more than one occasion, with Viet-Nam and Iraq as the extant examples,[12] that not only is secret intelligence easy to ignore and manipulate, but a reliance on secret intelligence can lead to a "shutting out" of overt common sense and open sources of information.[13]

Consider this, Daniel Ellsberg lecturing Henry Kissinger:[14]

> The danger is, you'll become like a moron. You'll become incapable of learning from most people in the world, no matter how much experience they have in their particular areas that may be much greater than yours [because of your blind faith in the value of your narrow and often incorrect secret information].

OSINT – intelligence that is publicly disseminated – is the single best antidote to the pathologies of secret executive power.

OSINT and the larger customer base for intelligence

Most citizens, and most legislators, assume that national intelligence or corporate intelligence is in the service of every part of the government, or every part of the corporation. This is not actually the case. In the USA, specifically, the focus continues to be on "secrets for the President," and on a few "hard targets" considered to be of the gravest possible concern – China, Cuba, Iran, North Korea. Within corporations, the emphasis is on serving the Chief Executive Officer (CEO). Consider the following questions as both a litmus test for intelligence managers, and as a broad definition of the possibilities for OSINT. To be explicit: every single customer ignored by the mandarins of secrecy or the sycophants to the CEO is a customer for OSINT.

- Do you believe that secrets are the ultimate form of knowledge, or do you believe that all sources including open sources should be brought to bear on decision-support?
- Do you believe that intelligence should focus only on the gravest of threats, what some call the "hard targets," or do you believe there is merit to "global coverage," seeking to monitor and understand all threats at some minimal mandatory level of detail?
- Is intelligence something that should be done only for the leadership, or should intelligence support – decision-support – be provided to agency heads, department heads, and even the individuals in the field, the front line that interacts with the real world?
- Is federal or corporate level intelligence only for the members of the federal government or the corporate headquarters, or should it support state and local jurisdictions, or subsidiaries?

OSINT and the levels of analysis

It is in the above context that we can conclude this overview by stating without equivocation that OSINT must be provided to all levels of any enterprise. This about empowering every individual, every segment of the enterprise, with decision-support (see Figure 10.4).

OSINT and coalitions

Although the concepts and doctrine that I have been developing for eighteen years recognize the seven tribes of intelligence as distinct historical, cultural, intellectual, and direct-access entities, it is the military and the concept of the military coalition that really serves as the spinal cord and nervous system for "harnessing the distributed intelligence of the Whole Earth."

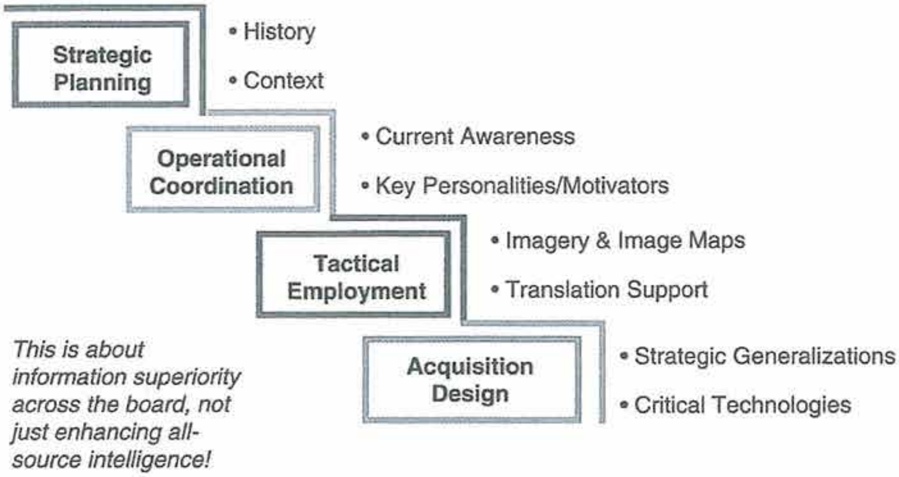


Figure 10.4 OSINT and the four levels of analysis

Within the USA, as within most countries, the military is consistently the most professional, the most disciplined, the most structured, and the most reliable organization. It is also the only one that treats Command and Control, Communications, Computing, and Intelligence (C4I) as a distinct discipline with its own Military Occupational Specialty (MOS) for each aspect.

It is a fact that the USA is simply not capable of fielding sufficient citizens with sufficient language and foreign area qualifications. Given the rapid rate at which available information doubles (a rate that will accelerate as hand-held devices become the instrument of choice, and are used to register photographs, videos, voice recordings, and text inputs from tens of millions operating in all languages, all the time), there is only one possible solution for mastering "all information, all languages, all the time." We must provide our coalition partners, and particularly our military coalition partners, with the means to digitize, translate, and analyze (using both automated tools and their own unique human expertise) all information of mutual interest, and we must provide a global Information Arbitrage™ capability that enables all coalition partners, each responsible for harnessing and nurturing their respective seven tribes, to participate in what I call the Open Source Information System – External (OSIS-X). Bi-lateral intelligence-sharing may still predominate in the secret world, but in the open source world, it is M4IS – multi-lateral sharing – that will define the common approach.

OSINT and saving the world

C.K. Prahalad has taught us that our government and business focus to date, on the one billion richest peoplé on the planet, who represent a one-trillion-a-year marketplace, is short-sighted. His brilliant book, *The Fortune at the Bottom of the Pyramid*, makes the important point that the five billion poorest people on the planet, because of their numbers and despite their low wages (an average of $1,000 a year, with half that number earning as little as $1 a day), actually represent a four-trillion-a-year marketplace – in short, a marketplace four times larger than the one that is active today.

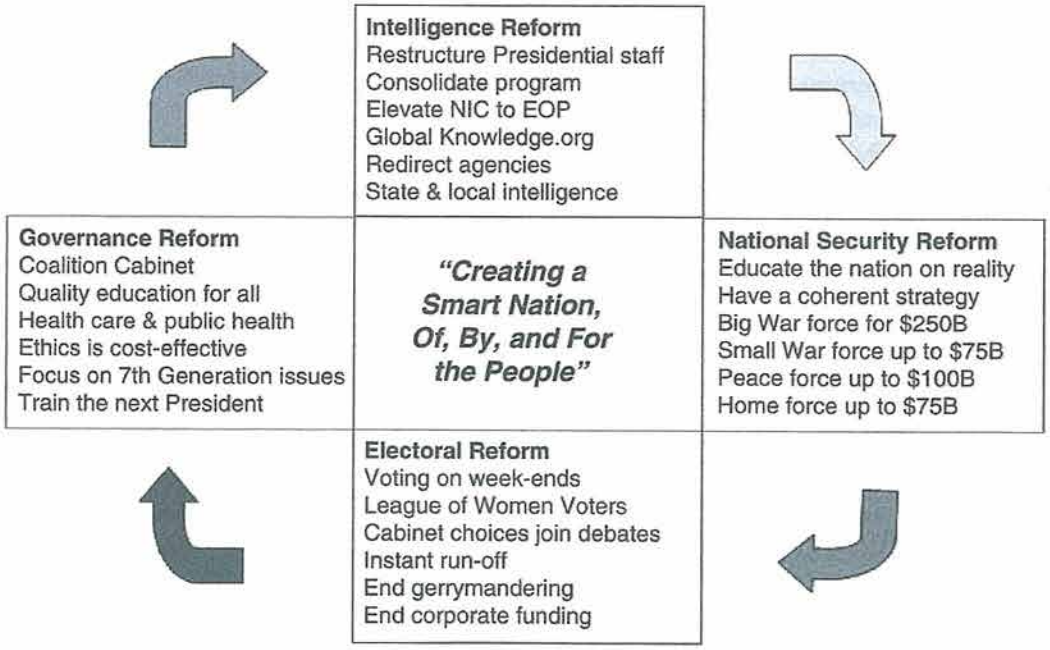
It was not until I absorbed the wisdom of C.K. Prahalad that I understand that OSINT can help the poor cut costs, reduce disease, improve health, and increase revenue. It is now possible to show religions, labor unions, and civil societies how to leverage the Internet and low-cost hand-held devices (instead of the more expensive laptops or personal computers) to apply OSINT from the "bottom up," and consequently to double or triple revenue at the bottom of the pyramid. The creation of sustainable indigenous wealth is without question the single fastest way to save the world from itself.

OSINT as a transformative catalyst for reform

America has been adrift for some time. The "me" generation spawned the disengaged generation, and we suffer now from the twin curses of an uneducated public that is also inattentive to its civic responsibility. This affects the rest of the world. It prevents us from keeping our politicians and corporate leaders honest, and its spawns terrible mis-adventures undertaken on the basis of ideological fantasies, without due policy process, or any semblance of a coherent affordable sustainable grand strategy. There is hope. See Figure 10.5.

Electoral reform, which could be inspired by multiple compounding failures of any administration across the board, or alternatively by a more aggressive practice of collective intelligence among the public, could lead to governance reform. A coalition government could demand that intelligence reform be substantive and comprehensive. This would have the happy outcome of imposing national security reform, which would not only reduce America's risk around the world, but would reduce the cost of the heavy-metal military, and free up resources for waging peace. From peace will follow prosperity. The low-cost, high-return value proposition from OSINT cannot be exaggerated.

Alvin and Heidi Toffler have focused in the manner in which information is a substitute for violence, for capital, for labor, for time and space. Others followed, including Thomas Stewart in *The Wealth of Knowledge* and Barry Carter in *Infinite Wealth*.[15] This is *real*.



Intelligence Reform
Restructure Presidential staff
Consolidate program
Elevate NIC to EOP
Global Knowledge.org
Redirect agencies
State & local intelligence

Governance Reform
Coalition Cabinet
Quality education for all
Health care & public health
Ethics is cost-effective
Focus on 7th Generation issues
Train the next President

"Creating a Smart Nation, Of, By, and For the People"

National Security Reform
Educate the nation on reality
Have a coherent strategy
Big War force for $250B
Small War force up to $75B
Peace force up to $100B
Home force up to $75B

Electoral Reform
Voting on week-ends
League of Women Voters
Cabinet choices join debates
Instant run-off
End gerrymandering
End corporate funding

Figure 10.5 OSINT as a transformative catalyst for reform

Open sources of information[16]

Open sources of information consist of the following general categories:

- Traditional media sources
- Commercial online premium sources
- Other niche commercial online sources
- Gray literature (limited edition locally available information)
- Overt human experts
- Commercial imagery and geospatial information
- The Internet and the world wide web (including emails and voice calls)

Open source software and software for exploitation

As a general statement, open source software is one of the five "opens" that will converge to create the World Brain. The others are, apart from OSINT, open (electromagnetic) spectrum, open access copyright, and open hypertext document system (OHS). The following standards are emergent as enablers of M4IS while still compliant with copyright or other individual caveats desired by the originator or owner of the information:

• RDF	Resource Description Framework
• OWL	Web Ontology Language
• SOAP	Simple Object Access Protocol
• OHS	Open Hypertextdocument System[17]
• XML Geo	eXtended Markup Language Geospatial
• IEML	Information Economy Meta Language.

There is no one offering that meets the need for a fully integrated analyst toolkit. This is partly because of the lack of agreement on standards in the past, and partly because of the lack of coherence in government and corporate contracting, where the emphasis has been on hardware and proprietary software instead of generic functionality and ease of data integration. The good news is that newly available offerings such as CISCO's Application Oriented Network (AON) are eliminating middleware, at the same time that Google's innovative approach to commodity storage has eliminated configuration management and back-up costs, while also reducing the cost for efficient global distributed storage and fast retrieval to one-third of the industry standard. Below are listed the desktop computing functions established by the Office of Scientific and Weapons Research at the Central Intelligence Agency (CIA) in 1986 as essential for analysis (see Figure 10.6).[18]

Open source services

Open source services include collection, processing (inclusive of man-machine translation), and analysis (inclusive of statistical or pattern analysis). When contracting for OSINT services, it is very important to evaluate the capability from the bottom-up (actual indigenous or localized capabilities to collect all information in all languages all the time) rather than the traditional and unprofessional way, which throws money at large contractors who then "fake it" and keep the

- Revision tracking, RT review
- Desktop publishing
- Graphics/multimedia production
- Collaborative work
- Notetaking & organizing ideas
- Structured argument
- Interactive search & retrieval
- Graphic map-based visualization
- Modeling and simulation
- Clustering & linking of data
- Statistical analysis for anomalies
- Detection of changing trends
- Detection of alert situations
- Easy digitization of hard copy
- Automated language translation
- Processing of images, signals
- Automated data extraction
- Data standardization/conversion

Figure 10.6 Fundamental functions for online analysis

bulk of the money for themselves. Generally when contracting for professional OSINT services, a good rule of thumb is to earmark one-third of the money for raw information collection, one-third for small businesses providing world-class translation and machine analysis services, and one-third for in-house or on-site analysts and related facilities.

The open source intelligence cycle

The open source intelligence cycle consists of the following steps that can be summarized by remembering "the four D's" of Discovery (Know Who Knows); Discrimination (Know What's What); Distillation (Know What's Hot); and Dissemination (Know Who's Who).

- Requirements definition
- Practical triage
- Collection (FIND free, GET free, BUY cheap, TASK dear)
- Processing and exploitation
- Analysis and production
- Security
- Dissemination and evaluation (Feedback).

The OSINT intelligence cycle cannot make up for pathological mind-sets (including ideological fantasy and political corruption) or poor management.

OSINT has one advantage over the other sources: its exposure to millions of pairs of eyeballs. As it commonly understood in the open source software world, put enough eyeballs on it and no bug is invisible.[19] OSINT also offers analytic frames of reference that have stood the test of time.[20]

Another misconception relates to production. Too many people misconstrue reports and page counts as "production" when in fact production does not consist simply of reports and page counts, but also includes link tables, distance learning, and professional networking. Figure 10.7 illustrates how one activates OSINT using the Internet.

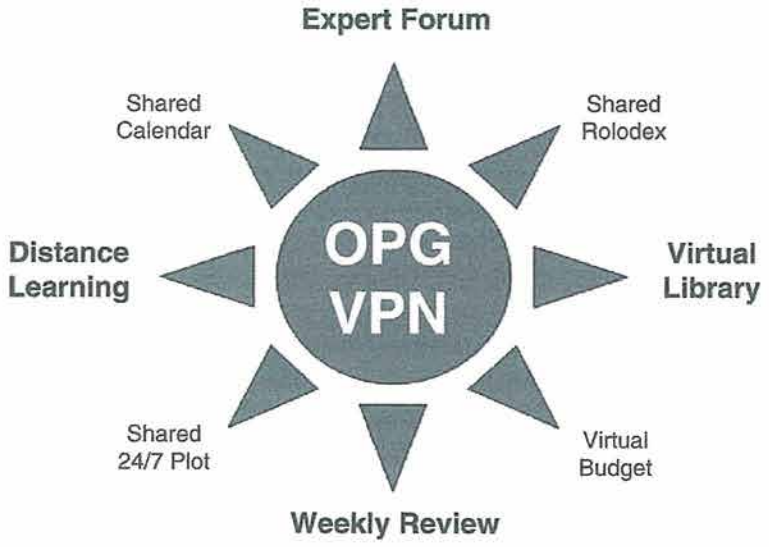


Figure 10.7 World Brain operational planning group virtual private network

The common mistake that most vendors of OSINT make is to confuse the weekly report or database-stuffing with "answering the mail." In fact, the weekly review is the foundation for a more complex process that requires each of eight distinct *iterative and interactive* capabilities to be present at all times.

OSINT is a continuous process of collection, processing, analysis, sharing, feedback, and expansion. Unlike secrets (for a spy, a secret shared is a secret lost), OSINT is enhanced, strengthened, validated, and monetarized by sharing.

At root, OSINT is about smart people creating smart organizations by sharing the burden of conceptualizing requirements, collecting all information in all languages all the time, doing multi-cultural inter-agency analysis, and then producing credible reliable intelligence that is actionable – it is useful and it leads to constructive outcomes. OSINT crosses all boundaries, and in so doing, brings us all closer together and helps us to both understand and to address common problems at every level of community and governance. OSINT saves lives, time, and money.

Applied open source intelligence

> Intelligence must be able to tell us, down to individual personalities and neighborhoods, "who," "where," and "how much" of "what" is needed, and whether what has been applied has been effective. If it doesn't know, it must have assets able to obtain and report the information within six hours of demand.
>
> (General Al Gray, Commandant, US Marine Corps)

When Dr Stephen Cambone, the Undersecretary of Defense for Intelligence, said in January 2004 that he needed universal coverage, 24/7, in all languages all the time, he was the first person at the highest levels of the US Government to formally adopt what General Al Gray recommended in 1988.[21] Sadly, despite various Commissions including the 9–11 Commission, as of this date the US Government is still not serious about open source intelligence.[22]

There is a simple reason for any leader to apply OSINT. It offers the best possible return on investment (ROI) for whatever resources – be they man-hours or dollars or Command interest – that can be earmarked for this emerging discipline. OSINT is the best possible way for any mission area specialist or professional to enhance their knowledge and increase their influence.

Open source intelligence tradecraft

This section simply itemizes key elements of tradecraft that are explained in more detail, with diagrams, in the *SOF OSINT Handbook*.

- *The Expeditionary Factors Analysis Model.* This model distinguishes between the four levels of conflict (strategic, operational, tactical, and technical) and the three interactive domains for conflict, military, civil, and geographic. The model also defines degrees of difficulty for the various mission areas as well as how the threat changes depending on the level of analysis.
- *The Revolutionary Analysis Model.* This model, for which a detailed analytic framework is available, distinguishes between political-legal, socio-economic, ideo-cultural, techno-demographic, and natural-geographic conditions, along a spectrum of psycho-social evaluation domains.
- *Analytic tradecraft.* Jack Davis is the *de facto* dean of the US national intelligence community's analytic cadre. The purpose of analysis is to help key individuals make intelligent decisions. The references should be read in their entirety.[23]
- *Social networking and expert networks.* The concept of "six degrees of separation,"[24] and the use of formal citation analysis,[25] will dramatically expand any analyst's effectiveness.

Mission relevance of open source intelligence

This section must of necessity be abbreviated. Twenty-five pages replete with search examples using only Google are available in the free *SOF OSINT Handbook*.

- *Strategic historical and cultural understanding* addresses the critical importance to any mission of going back in time to understand the history of the region, the history of foreign powers as well as the US in the region, and the history of anti-americanism in the region. If there is one thing we cannot afford when going in-country, it is to be delusional about just where we stand as we go about trying to win hearts and minds or as we capture single hostile individuals in a context where we do not realize the odds are stacked against us. *The greatest threat to any mission is not armed forces but rather hostile observers.* Understanding history and culture is fundamental.
- *Operational understanding for campaign planning* connects open sources of information to the theater level of warfare, and helps develop an understanding of open sources in relation to the current situation. Regional power sources, status discrepancies among tribal groups, change agents that are present or emergent, internal security and stability issues (water, food, energy, health, crime, for example) are all essential to understanding the weak links in a current social structure that we can either leverage for operational advantage, or must be aware of to avoid operational failure.
- *Tactical sub-state understanding for unit effectiveness* gets to the heart of the matter for units that will be working in-country. This chapter focuses on tribal orders of battle down to the village and elder level, on key leaders and value-based biographies, on understanding

the local media and how groups and individual communicate with one another, and finally, on content analysis – understanding *their* PSYOP themes.

- *Technical understanding for policy, acquisition, and operations* begins with an introduction to the *NATO Open Source Intelligence Handbook*, which is the technical reference and companion to this volume, and then provides a very brief overview that relates open sources of information to policy, acquisition, and operations in general. One of the great things about OSINT is that it can be used to study domestic US policy debates as well as allied debates. Understanding the players, both friendly and third party, and understanding how the players are perceived locally, is at the heart of any successful CA or PSYOP endeavor. OSINT can also enhance acquisition, and help decide what to leave on the pier and what to take along on the mission.

Mission area applications

Thirty-three pages with additional detail are in the *SOF OSINT Handbook*.

- *Civil affairs* can use OSINT in relation to human intelligence (understanding the demographics, the socio-economic environment, displaced persons, and crime, among other topics); to technical intelligence about the local command and control, communications, computing, and intelligence environment, the infrastructures of transportation, power, and finance; to welfare intelligence (water, food, medical); cultural intelligence about protected or restricted targets, and liaison intelligence.
- *Psychological operations* can use OSINT in relation to strategic, operational, and tactical campaign plans; revisits the mapping of themes in play, especially anti-US themes; the original collection and testing of themes for possible US play, and the litmus test for successful PSYOP: does the message produce actionable intelligence from indigenous volunteers?
- *Target analysis* discusses how OSINT might fulfill team needs in the absence of classified intelligence support, to create a detailed description and vulnerability assessment, evaluate the natural environment and the human environment, and carry out route-planning.
- *Terrain analysis* uses OSINT to establish key factors relevant to special aviation and covert ground movement, in part by leveraging commercial and Russian military combat charts, commercial imagery, and alternatives for terrain reconnaissance including unmanned aerial vehicles and indigenous scouts.
- *Weather analysis* uses OSINT as a means of rapidly getting to the basics of temperature, visibility and timing of sun and moon, wind, and inclement weather.

In addition to the *SOF OSINT Handbook*, see the Quick Links Guide for the Military Analysis, included in the one-page list of links at www.oss.net/BASIC.

Conclusion

Money matters

Funding trade-offs. As our larger world comes to grips with the end of cheap oil, the end of free clean water, the rise of pandemic disease, the twin deficits and rampant militarism of the USA under the Bush–Cheney Administration, the bottom line is clear: we have no slack left, we are at a tipping point, every mistake could be fatal. It is no longer adequate to muddle through, draw down on savings, or "make the best of it." Any manager, any person, that does not invest the time and as needed the money to make informed decisions using OSINT, is derelict in their duty to their employers and themselves. OSINT is now an established discipline required for "due diligence." Perhaps more importantly, information is a substitute for time, money, labor, and space. Practicing OSINT is a way of printing your own money! Practicing OSINT is also a means of restoring power to the people, allowing them to better hold accountable their policymakers and corporate executives all too inclined to manipulate or ignore secrets, or claim special knowledge that does not exist, as a means of justifying actions and expenditures that are not in the public interest.

Contracting mistakes. As a general comment, we have found that the biggest failure among both government and private sector clients is that of almost total ignorance with respect to the diversity and quality of open source services, and most especially of those offered by foreigners in their own localized environments. Even those organizations that have the wit to contract for a variety of open source services generally do not have a single focal point nor do they attempt to monitor best prices and best practices. The worst possible mistake is to attempt to procure OSINT from a major defense corporation that specializes in massive expensive projects to deliver technology that often does not work and "butts in seats," rather than niche expertise or direct access to all information in all languages all the time. It is also a mistake to contract for the delivery of OSINT without making provision for a working requirements process that will save time and money by getting the questions right in the first place, or to contract for the delivery of OSINT in hard-copy, without making provision for its delivery in a form that will allow its easy dissemination throughout the sponsoring organization's network. A more nuanced contracting mistake is to avoid seeing that information, once purchased, has a tangible value that can be used to barter for more information. Copyright issues notwithstanding, a coherent program for sharing information with varied members of the seven tribes in one's own home country, and with counterpart organizations from other countries, will generally produce a ten to one return on investment – ten new useful pieces of information for each single piece of information that is shared broadly.

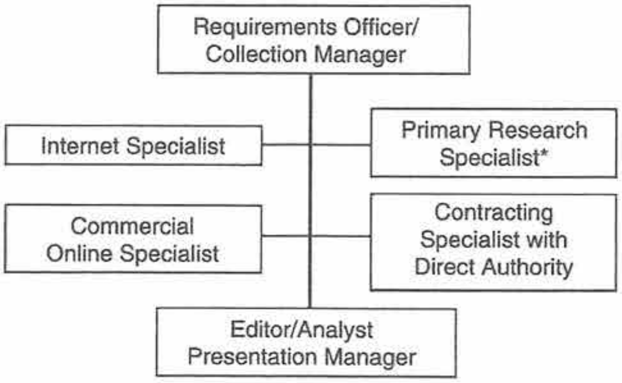
Metrics for measuring return on investment. There are three valuation metrics that can be applied in evaluating the role of OSINT in any organization's Information Operations (IO).

- *Cost of secrecy.* Transaction costs are higher. Classification reduces competition from domestic and foreign providers of better information. Functional costs come from non-interoperability and operational disconnects. Clients tend not to access all that is offered because of the obstacles imposed by handling secret information (e.g. reading on a trip).
- *Relative value.* Is the OSINT "good enough" now? Does it provide, in context, "good enough" understanding to move forward? For the decision at hand, it is "good enough" to allow the decision to be made? Can the information be shared and thus engage other stake-holders?
- *Return on sharing.* Does this information, shared openly, attract other information that is equally useful? Does this information, shared openly, reach others who have a "need to know" and consequently include them and engage them in an expanded network for mutual benefit?

Commercial strategy. Dr Joseph Markowitz, the only truly competent manager of open source information endeavors within the US Intelligence Community, published a commercial strategy prior to resigning from government service. It has yet to be implemented.[26]

Budget and manning recommendations. Detailed proposed budgets are online[27] for a national Open Source Agency (OSA), a theater Multinational Information Operations Center (MIOC) and network, and a subordinate commercial imagery and geospatial procurement plan. It remains, then, to simply illustrate a standard OSINT "cell" such as could be added to any corporate or government library, with the observation that OSINT should be accomplished in three tiers:

- If it can be done online in less than 15 minutes, the analyst should do it.
- If it will take 15–60 minutes, or require specialized knowledge, the OSINT cell should receive the task (see Figure 10.8).
- If it will take more than 60 minute or require very specialized knowledge or direct access, it should be out-sourced to exactly the right source or service, by the OSINT cell, which should be expert at best prices and best practices for all sources in all languages all the time.


Requirements Officer/
Collection Manager
Internet Specialist
Primary Research Specialist*
Commercial Online Specialist
Contracting Specialist with Direct Authority
Editor/Analyst Presentation Manager

*Specializes in methods for finding and interviewing exactly the right individuals.

Figure 10.8 Standard OSINT cell

The value of sharing

We have, as J.F. Rischard puts it so well in *High Noon: 20 Global Problems, 20 Years to Solve Them*,[28] reached the point of no return. OSINT is relevant to individual security and prosperity; to organizational and national security and prosperity; and to global security and prosperity. He writes about sharing our planet, sharing our humanity, and sharing our rule book. Tom Atlee, founder of the Co-Intelligence Institute and author of *The Tao of Democracy: Using Co-Intelligence to Create a World that Works for All*[29] adds another group to these three groups: sharing our wisdom. Sharing our wisdom. That is what distinguishes OSINT from the secret collection disciplines, and that is what distinguishes the role of OSINT in the world of analysis: it can be shared without restriction. OSINT *is* democracy. OSINT *is* moral capitalism. OSINT *will* make our lives better and offer hope to future generations. *E Veritate Potens*.[30]

References

Visit http://www.oss.net and see especially http://www.oss.net/BASIC. See also the books by Robert Steele:

On Intelligence: Spies and Secrecy in an Open World (Foreword by Senator David Boren, D-KS), first published in 2000.

The New Craft of Intelligence: Personal, Public, & Political – Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption (Foreword by Senator Pat Roberts, R-KS), 2002.

Peacekeeping Intelligence: Emerging Concepts for the Future (contributing editor, Foreword by Dame Pauline Neville Jones), 2004.

Information Operations: All Information, All Languages, All the Time – The New Semantics of War & Peace, Wealth & Democracy (Foreword by Congressman Rob Simmons, R-CT-02), 2006.

The Smart Nation Act: Public Intelligence in the Private Interest (Foreword by Congressman Rob Simmons (R-CT-02), sponsor of The Smart Nation Act), 2006.

Acronyms

Acronyms are included in the Glossary to this *Handbook*.

Notes

[1] The executive summary is a precise replication from the *NATO Open Source Intelligence Handbook* (November 2001), which remains the standard in the field. Drafted by the author, with important refinements from LCdr Andrew Chester, RN Canada, and under the leadership of Capt. David Swain, RN, United Kingdom, this volume was approved by General William Kernan, USA, then Supreme Allied Commander Atlantic. The NATO documents and other essential references on OSINT, including the original OSINT Executive Overview, are easily accessible by going to http://www.oss.net/BASIC. This chapter is of necessity a very summative rendition of the 20,000 pages of accumulated knowledge in the Archives at http://www.oss.net, most of which can be accessed in a structured manner via the above URL.

[2] The most important new concepts to receive traction since the release of the NATO documents are those of the Seven Tribes, Collective Intelligence, and the World Brain. The seven tribes, each of which has unique access and perspectives, are those of government, military, law enforcement, business, academic, ground truth (media and non-governmental organizations), and civil (citizens, labor unions, and religions). Collective Intelligence and the World Brain are discussed in Note 3.

[3] The Swedish concept was advanced at the third Peacekeeping Intelligence Conference sponsored by the Folke Bernadotte Academy and Swedish National Defence College under the direct leadership of the Supreme Commander, 4–6 December 2004. The Co-Intelligence Institute was founded by Tom Atlee, author of *The Tao of Democracy: Using Co-Intelligence to create a world that works for all* (The Writer's Collective, 2003). Howard Rheingold, former editor of *The Whole Earth Review*, is the author of *Smart Mobs: The Next Social Revolution* (Perseus, 2002) as well as seminal books on *Tools for Thinking, Virtual Reality*, and *Virtual Communities*. James Surowiecki is the author of *The Wisdom of the Crowds: Why the Many Are Smarter than the Few and How Collective Wisdom Shapes Business, Economies, Societies, and Nations* (Doubleday, 2004). Key works on the emerging World Brain include those of H.G. Wells, *World Brain* (Admantime, 1994 from 1938); Pierre Levy, *Collective Intelligence: Mankind's Emerging World in Cyberspace* (Plenum Trade, 1997); Willis Harman, *Global Mind Change: The Promise of the 21st Century* (Noetic Sciences, 1998); and Howard Bloom, *Global Brain: The Evolution of Mass Mind From the Big Bang to the 21st Century* (John Wiley, 2000).

[4] This term was developed by Dr Stevan Dedijer, a Swede who was born and died in Croatia (former Yugoslavia), widely recognized as the father of modern business intelligence. He led fifteen Swedes to the first Open Source Intelligence Conference in 1992, where he made a passionate plea for government attention to this vital independent discipline.

[5] Dr Joseph Markowitz, the first and only Director of the Community Open Source Program Office (COSPO) before it was destroyed by the Community Management Staff (CMS), devised this important distinction between OSINT such as can be done by private sector practitioners, and OSINT as validated by government analysts with full access to classified sources and methods.

[6] In "The Strategic Use of Open-Source Information," *Studies in Intelligence* 45/3 (2001), pages 67–71.

Dr Gannon is, with Dr Markowitz and Dr Gordon Oehler, one of a tiny handful of all-source managers who understand the full range of OSINT. However, those who remain within CIA, well-intentioned as they may be, are so mired in legacy mind-sets, legalities, security encumbrances, and general malaise as to be pathologically ineffective at OSINT, even when trying to support only the small cadre of analysts within the CIA. A careful reading of all public references to OSINT by CIA managers shows a delusional focus on information technologies that have yet to be put on the analysts' desktops, while defining "sharing" as being limited to those with access to Top Secret "system-high" clearances and terminals.

[7] Detective Steve Edwards of Scotland Yard, honored by the Queen for his accomplishments in applying OSINT to law enforcement, says this: "I now consider POLINT [Police Intelligence] to be a sub-category of OSINT as the collection and sourcing are largely the same. Anything else needed is largely supplied using other disciplines. OSINT is also the only real way for most interested parties to collect the information without recourse to methods that could be seen as over-intrusive; bearing in mind who the targets might be." Professor Hugo Smith, in his seminal article on "Intelligence and UN Peacekeeping" in *Survival* 26/3 (Autumn 1994), says: "The concept of 'UN intelligence' promises to turn traditional principles of intelligence 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." Reprinted in Ben de Jong et al., *Peacekeeping Intelligence: Emerging Concepts for the Future* (OSS, 2003).

[8] Dr Robert Garigue, formerly a top practitioner of Information Warfare as a Canadian naval officer, has articulated the new semantics of war and peace, wealth and democracy, in his Technical Preface to the author's book on *Information Operations: All Information, All Languages, All the Time* (OSS, 2006). His views are well in advance of existing doctrine.

[9] The author is indebted to Admiral Bill Studeman, USN (Ret.), former Deputy Director of Central Intelligence (DDCI), former Director of the National Security Agency (NSA), and former Director of Naval Intelligence (DNI), who in his post-retirement years has become a master of IO and all that this implies. In the age of information, IO is the manifestation of "total war" and the need – not yet realized – to harness every source of national power including an educated citizenry and informed politicians to further national advantage.

[10] (United Nations, 2004), The endeavor benefited from the participation of the Honorable LtGen Dr Brent Scowcroft, USAF (Ret.), former national security advisor to President George Bush. Terrorism is either fifth on this list or seventh if the first is counted as three. The report, 262 pages in length, can be seen at http://www.un.org/secureworld/report2.pdf.

[11] While not the focus of this chapter, it merits comment that according to the Commission on the National Imagery and Mapping Agency, in a report published in December 1999, most of the intelligence money is spent on esoteric collection systems, and almost none at all is spent on actually making sense out of the collected information.

[12] For Viet-Nam, the single best reference on cooking the books and spinning the truth is George Allen's *None So Blind: A Personal Account of the Intelligence Failure in Vietnam* (Ivan R. Dee, 2001). On the topic of Peak Oil, 9–11, and Iraq, there are numerous books, of which three stand out: James Bamford, *A Pretext for War: 9/11, Iraq and the Abuse of America's Intelligence Agencies* (Doubleday, 2004); James Risen, *State of War: The Secret History of the CIA and the Bush Administration* (Free Press, 2006); and Michael C. Ruppert, *Crossing the Rubicon: The Decline of American Empire at the End of the Age of Oil* (New Society, 2004). Many other books address various aspects of how 9/11 represented both a break-down of secret intelligence and a celebration of ideological fantasy unchecked by responsible oversight.

[13] During the eighteen years of my campaign to secure added funding for and emphasis on OSINT, open source information has been derisively referred to as "Open Sores" by nominally intelligent but foolishly unprofessional managers and some analysts at the Central Intelligence Agency (CIA). Even the so-called open source professionals in the Foreign Broadcast Information Service (FBIS) have refused to be serious about anything other than mainstream broadcast media until allies of OSINT finally got an Open Source Agency into the 9/11 Commission Report (page 413). The mind-sets within CIA and its runt orphan FBIS (now nominally a DNI-level Open Source Center) have not yet matured on this topic.

[14] Daniel Ellsberg, *Secrets: A Memoir of Vietnam and the Pentagon Papers* (Viking, 2002). The three pages on the pathological effects of falling prey to the cult of secrecy, on pages 237–239, should be forced rote memorization for all who receive clearances.

15 *PowerShift* (Bantam, 1990). Stewart (Currency, 2001). Carter (Butterworth Heineman, 1999).

16 The next four sections are superficial in relation to the *NATO Open Source Intelligence Handbook.* There is no substitute for downloading and studying that reference as well as the *NATO Open Source Intelligence Reader* and the NATO guide to *Intelligence Exploitation of the Internet.* These and other key references are freely available at http://www.oss.net/BASIC.

17 This is the only standard that may not be readily apparent when this chapter is published. Invited by Doug Englebart, inventor of the mouse and hypertext, this standard enables linkage of related content to take place at the paragraph level, which also allows copyright compliance to be executed at the paragraph level, for pennies instead of dollars.

18 Diane Webb, under the leadership of Dr Gordon Oehler, developed *CATALYST: A Concept for an Integrated Computing Environment for Analysis* (CIA/DI SW 89–10052, October 1989). To not have this now, close to eighteen years after precise requirements definition, tells us clearly of the sustained pathos of US Intelligence Community "leadership." Follow link at www.oss.net/HISTORY.

19 The actual quote is "given enough eyeballs, all bugs are shallow." This is generally attributed to Eric Raymond, is known as the Linus Law, and is associated with the Free/Open Source Software (F/OSS) movement.

20 See the analytic references at http://www.oss.net/BASIC.

21 General Al Gray, "Global Intelligence Challenges of the 1990's," *American Intelligence Journal* (Winter 1988–1989). At www.oss.net, Google for title.

22 The appointment of an Assistant Deputy Director of National Intelligence for Open Source (ADDNI/OS) on 5 December 2006 was a step in the right direction, but this individual has no program authority, no money, and no staff. Meanwhile, the Open Source Center at the Central Intelligence Agency, a cosmetic re-definition of the Foreign Broadcast Information Service (FBIS), has absolutely no likelihood of being relevant to anyone outside CIA in the next ten years. Fortunately, the Open Source Information System (OSIS) is a national-level system belonging to the Senate-confirmed Chief Information Officer for the Director of National Intelligence, an Air Force Major General who understands that the key to open source exploitation is sharing rather than secrecy, standards rather than security. Applied OSINT will flourish outside the secret intelligence world – to the extent that OSINT is ably developed by the US Intelligence Community, it will be through OSIS embracing the 90 nations forming the Coalition, rather than through the OSC/FBIS. We continue to lack a national Open Source Center under the auspices of the Department of State, a sister agency to the Broadcasting Board of Governors. In as much as 90% of the open source information we wish to gain access to is controlled by individuals who have no wish to be associated with the US Intelligence Community, US OSINT will not be effective until a national agency is established under diplomatic auspices – consequently, US IO will also be pedestrian absent that agency.

23 The compendium, the "New Rules" chapter from *The New Craft of Intelligence*, and a lecture on "Analysis: Making Magic" are all accessible via www.oss.net/BASIC.

24 Stanley Milgram, "The Small World Problem," *Psychology Today*, 1967. Google "small world problem."

25 Citation analysis is generally done for English-language information using the *Social Science Citation Index* and the *Science Citation Index*. Other countries, such as China, are now creating their citation analysis directories. Any analyst who does not know who the top 100 people in the world are for their respective area of interest should go to their library and ask them to do a DIALOG RANK Command for their topic. It will cost about $500. The superior analyst will then obtain biographies for each of those individuals, engage with all of them, and through them, identify the top 100 individuals that are not published (e.g. government and non-government officials).

26 See the link under Policy and Investment at www.oss.net/BASIC.

27 Ibid.

28 (Basic, 2002). The author is Vice President for Europe of the World Bank.

29 (The Writer's Collective, 2003). Observation made in a personal communication (electronic mail) of 18 March 2006. The Co-Intelligence Institute merits more attention and support.

30 This is the motto for OSS.Net, Inc., and before that for the Marine Corps Intelligence Command which the author helped create. It means "from truth, power" or literally, "one is made powerful by the truth." Thus does OSINT contribute to the power of every individual regardless of their race, nationality, religion, or station in life.