APPENDIX C

ACCESS:
Theory and Practice of Intelligence in the Age of Information

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

95% de l'information dont une entreprise a besoin peut s'acquirir par des moyens honorables.

Henry Stiller, Director General
Histen Riller, Societe Civile

Executive Summary

Point #1: In the Age of Information, "intelligence" is less a matter of penetrating secrets, and more a matter of separating useful information from the flood of open information that is available legally and cheaply; *electronic sources are especially useful.*

Point #2: In combination, the economic and political cost of industrial espionage, or penetrations of other governments to divine "plans and intentions", are insupportable when contrasted with the benefits of open source intelligence (OSCINT).

Point #3: The concept of "central" intelligence cannot survive in the Age of Information. By focusing on OSCINT, a Nation can mobilize each of its knowledge sectors, and turn the entire Nation into a "virtual" intelligence agency with far greater collection, processing, and action capabilities than are provided by the existing bureaucracies dedicated to national and defense intelligence.

Point #4: Comprehensive national knowledge strategies must provide for connectivity, content, culture, coin, and C4 security: the "Five C's".

Table of Contents

2. Discussion. Role of intelligence and "virtual" intelligence; information as a substitute for capital and labor; possible investment strategy for information; political and economic cost of espionage; pre-publication/pre-secret windows of opportunity; speed advantages of open source exploitation.

3. Information Requirements and Player Identification. Priority versus gaps-driven collection; four major consumer groups of intelligence; refining the gaps-driven requirements process; model for consumer-oriented production; four major target groups for intelligence; four kinds of players in the open source arena.

4. Sources of Information and Methodology. Five distinguishing aspects of information sources; essential reorientation of intelligence toward open sources; privatization of intelligence; five elements of a national knowledge strategy.

5. Industrial Espionage, Sanctions, and Proscribed Information. U.S. views of Japanese and French; general attitudes about industrial espionage; sanctions; proscribed (prioprietary) information.

6. Analysis. Rules of the game have changed; competitive advantage has shifted from secrecy to openess; new "order of battle" needed for national intelligence; national knowledge strategy is a critical initiative; strategic opportunity for competitive advantage exists.

7. Action Requirements. Reinvent national intelligence; realign resources; establish a national information requirements council; establish open source focal points within United States and other countries.

8. References. Resume and selected publications; other works of importance; date of information.

1. Background

What is the issue? The issue of access has enormous importance for both the national security and the national competitiveness of any Nation.

> *The issue for the client is: how does a Nation achieve national security and national competitiveness in the Age of Information, and what does this mean to existing national policies on intelligence organization and the expenditure of public and private funds for information collection, processing, and dissemination activities.*

Changed "Rules of the Game. An understanding of the "sources and methods" which comprise "access" in the Age of Information is absolutely vital for top-level decision makers in both government and the private sector. Top-level decision-makers must understand that the "rules of the game" have changed, and that competitive advantage in the

Age of Information is dependent on the laws of cybernetics, not the laws of physics. Under the laws of physics, secrecy and the restriction of knowledge provided a temporary advantage. In cybernetics, openness and flexibility win.

Most great nations spend on the order of $20 billion to $30 billion a year on "intelligence", which is traditionally comprised of clandestine human intelligence, and technical collection of imagery and signals.

National Information Continuum. At the same time, most great nations have an "information continuum" (illustrated below) whose endeavors and products are going to waste...the capabilities of these elements of the national information continuum are not being exploited! This continuum represents, in a typical great nation, a $100 billion per year capability that is lying fallow.

K-12 Libraries PI/IB Government Intelligence

Universities Business Media Defense

Figure 1A. The National Information Continuum--Nine Sectors

NOTE: The above is an original representation that has been current in the literature for over a year. It is different from the more practical Sector Breakout because it reflects a focus on elements of the information continuum which do not--at this time--contribute significantly to national and defense research endeavors.

Four Information Categories. There are four "information categories" in the access arena. They are:

a. Open source or public information; within intelligence communities, this is known as open source intelligence or OSCINT. "Grey literature", literature which is unclassified and not proprietary, but produced in limited quantities for limited purposes, is included as an element of OSCINT. Open (unclassified) electronic information, such as that available through the INTERNET and related file servers and newsgroups, is also included in OSCINT. *The vast majority of scientific & technical intelligence is available through OSCINT, to include 600 scientific & technical journals that appear only in electronic form.*

b. Open proprietary information, discernable through open source investigation. This includes the reverse engineering of legitimately acquired products, and legally conducted "competitor intelligence". (Note: competitor intelligence is the globally accepted term for legal research efforts by businesses studying their competitor's products, organizations, and related matters.)

c. Closed proprietary information, available only through industrial espionage or

clandestine and technical penetrations of regulatory agencies.

d. Classified information, available only through clandestine human intelligence or technical (imagery or signals) intelligence.

Open Sources	Proprietary (Open)	Classified
Grey Literature	Proprietary (Closed)	

Figure 1B. The Four Information Categories

Three Characteristics of Value. The value of information is derived from three characteristics of the information: its substance or content; the context within which it is being considered by others; and the timing with which it is received.

> *The single most significant step an organization can take to increase the value of the information it is acquiring is to increase the speed with which the information is acquired and acted upon. This is also the most inexpensive step--but only if top management is willing to accept significant changes in doctrine and procedure.*

Speed as the Foundation for Security. The speed with which information moves and achieves value depends less on the information itself (the externality) and more on the degree to which the participating organizations are organized and aware of their requirements (the internality). Organizations are drowning in information because they have not learned to swim. They are not trained, equipped, or organized to collect, process, disseminate, and act upon information. The most important employees, the ones with the contextual understanding of the situation, are normally not empowered to act on information, and normally do not receive intelligence products.

Imbuing a national infrastructure with "speed" really means that a complete change is required in the way in which organizations relate to one another, and in the way in which managers relate to front line workers or action officers. The beauty of working with open sources is that it eliminates, in a single stroke, all of the political and legal, as well as the economic, constraints that characterize the sharing of classified information. We have been trying to water the desert with oil, instead of water.

Hard Copy versus Electronic Information. Finally, in discussing issues of access, it is important to understand the relative value of hard copy versus electronic information. Although hard-copy information far outweighs electronic sources in quantity, and particularly in relation to Third World sources, the electronic world is where "up and coming" technologists as well as "up and coming" leaders are communicating their most signficicant thoughts.

The electronic world is especially useful because it allows an enormous amount of research to be conducted from a single location, and also allows relatively anonymous browsing through other computers or commercially available databases. Hard-copy is an important secondary source, especially when investigating Third World and non-technical issues.

Third World Hard Copy "Cyberspace"

First/Second World Hard Copy INTERNET

Figure 1C. Hard Copy versus Electronic Information

2. Discussion

Role of Intelligence and "Virtual" Intelligence. There is no issue more important to a Nation in the Age of Information than that of the role of intelligence--not only of the role of the traditional national intelligence services, but also of the non-traditional "virtual" intelligence services which are represented by the other elements of the national information continuum.

> *A proper perspective on this matter, at the highest levels of both the government and the private sector, represents at least a $100 billion a year value. This is enormously important, not only because it will be the major policy area affecting the future of the Nation, but because it is relatively easy to achieve by realigning and coordinating existing capabilities and funds.*

Information as a Substitute for Capital and Labor. In the Age of Information, when information is the "first order" commodity, and information is a substitute for time, space, capital, and labor, the implications of this discussion are enormous. The fate of the Nation depends on a proper appreciation of this issue, and on adequate coordination between government and private sector leaders responsible for elements of the information continuum.

Possible Investment Strategy for Information. The four "information categories" in the access arena can be evaluated as follows:

-- Open source: 80% of what is required for sound decision-making, at 20% of the cost, in 20% of the time (relative to industrial espionage or classified collection). The value of open source information cannot be exaggerated.

-- Proprietary (open): 5% of what is required, for an additional 10% cost increment.

-- Proprietary (closed): 5% of what is required, for an additional 20% cost increment.

-- Classified: 10% of what is required, for an additional 50% cost increment.

|----------OSCINT (80%)----------|

PROPRIETARY (10%)
CLASSIFIED (10%)

Figure 2A. Possible Investment Strategy for Information

Political and Economic Cost of Espionage. It merits comment that industrial espionage in particular, but clandestine and technical intelligence as well, reflects a political risk, or a potential political cost, that is easily triple the economic cost--industrial espionage and classified penetrations are not only twice as costly as open source exploitation, they are also twice as likely to "explode" in the face of their sponsor.

Pre-Publication/Pre-Secret Windows of Opportunity. In the area of open source information, or open source intelligence (OSCINT), it is very important that decision-makers understand the levels of access in terms of time
--time is the vital aspect of cybernetics, and is the critical factor in national competitiveness:

Published sources are available to mass audiences at the same time--books are generally provided to the public years after they were actually written; articles generally months after they were written; and newspaper reporting days or weeks after being drafted..

"Grey literature" is available to specialized audiences at the same time, and to non-members after a period of time.

"Work in progress" in available to peer review groups and to specially equipped "outsiders".

"Pre-publication intelligence" is available to specially equipped outsiders who take the trouble to identify and cultivate selected sources of public information. This area is the "center of gravity" for those who seek to "reinvent" national intelligence.

Speed Advantages of Open Source Exploitation. There are two reasons why open source intelligence (OSCINT) is a vital area of concentration: the first is that most applied technology, including proprietary or classified technology, begins with open publications about its sub-elements, and it is often possible to piece together very good intelligence reports "at the source" while avoiding the risk of industrial espionage or clandestine operations against foreign targets. The second reason is that every "dual-use" technology to which export controls are eventually applied spends at least two years, and sometimes up to ten years, in "beta" development. The Department of Commerce, which has the lead in classifying dual-use technology, is generally two years behind actual market developments; this is particularly true in the software arena. Thus, the best time to capture a "secret" or a restricted technology, is during the two year "beta" window before it becomes a secret or is

restricted.

Real-Time Mind Link Beta Testing Traditional Sources

Work in Progress Gray Literature

Figure 2B. Speed Advantages in Open Source Exploitation

Refining one's open source intelligence (OSCINT) intelligence process to collect information in the pre-publication stage, by identifying and keeping in touch with key experts who provide advance looks at "works in progress", adds a further six months to a year of competitive advantage. *Electronic searching is the single most vital tool in identifying these experts "in time".*

3. Information Requirements and Player Identification

There are three ways of looking at the information playing field: by focusing on the four consumer groups for national intelligence; by focusing on the four warrior classes of the future; and by focusing on the sources of information. Each will be discussed in turn, together with a means of executing gaps-driven collection and consumer-oriented production.

Priority versus Gaps-Driven Collection. The information requirements arena is traditionally one which intelligence communities have not mastered. Too often they collect what is collectable, or obviously protected, and they rarely produce intelligence that is tailored to a specific customer or delivered "just in time". Information requirements are typically driven by gross priorities (e.g. the Soviets are priority one, the Chinese priority two), rather than by "gaps" or real requirements. This often means that Third World encyclopedic intelligence (most of which is unclassified), and economic or demographic intelligence vital to penetrating foreign markets, does not receive the attention it requires.

Four Major Consumer Groups of Intelligence. There are four specific groups of information customers that every intelligence organization should be serving, but generally does not, because it focuses on the very highest levels of government rather than on the subordinate levels where policy is actually created and actions are taken on a day to day basis.

a. Departmental planners and programmers, in every Department of government, not only in the national security arena, require both strategic generalizations (rather than a flood of detailed reports about tiny parts of many problems), and political-military information heavily laden with information about "plans and intentions".

b. Regional planners and programmers, including Ambassadors and Assistant Secretaries of every Department of government, require regional generalizations and very detailed mobility and market information. This is the customer group most likely to take

advantage of intelligence which focuses on opportunities for advantage, opportunities to prevent disaster or establish commercial gains before anyone else realizes there is a threat or an opportunity to be contested.

c. Ambassadors and corporate general managers in specific countries require both detail about the physical capabilities of their opponents or competitors, and very detailed evaluations of sustainability, availability, reliability, and or accuracy of competitor products. In the economic arena, intelligence about demographics and culture is more easily obtained, and more valuable, than internal corporate information about competing products. If you understand the BUYER's requirements, you do not need to collect every detail about competing SELLER's capabilities. This point merits elaboration: competitive advantage comes from satisfying the buyer, not from beating the opposing seller. It is far more important to understand every detail about what the buyer wants to buy, than attempting to understand opposing solutions.

d. System designers and project managers, and those at the most senior levels who make acquisition and investment decisions, generally receive adequate intelligence about technical details, but do not receive good intelligence (intelligence which is generally unclassified) about whether the system is really worth acquiring in terms of cost-value, competing means of meeting the requirement, cost of sustainability, and so on. For instance, most advanced nations have invested billions of dollars in fast-moving sophisticated systems and failed to establish the necessary communications and computer support to actually make those systems effective in the field.

System Designers Regional Planners

General Managers Department Planners

Figure 3A. Four Major Consumer Groups for Intelligence

Refining the Gaps-Driven Requirements Process. The greatest flaw in a priority-driven requirements process is that it is divorced from the day to day needs of the policy and action-level consumer. Priority-driven collection tends to err on the side of repetitive and "vacuum cleaner" collection against the highest priorities, and to completely disregard both encyclopedic and current intelligence requirements for targets which may be of a lesser priority in the "grand strategy" arena, but of vital interest at the operational and tactical levels. A gap-driven information requirements process will take its requirements each day (rather than through monthly or quarterly "priorities validation" meetings), both from the consumer of intelligence ("here is what I need to know tomorrow") and from the analyst ("here are the things I did not know in producing this report").

Model for Consumer-Oriented Production. The existing production model, at least in the United States, is based on "stove-pipe" production which is rarely as "all-source" as it could be (e.g. the National Security Agency produces reports drawn largely from signals

intelligence), and is also severely deficient because it focuses on specific countries, topics, or weapons systems--i.e. the production is defined by the target, not by the needs of the consumer. Below is illustrated a superior line of consumer-oriented products, most of which would be unclassified and whose contents would be primarily drawn from open sources of intelligence.

BASIC PRODUCTION: COUNTRY PROFILES. Integrate executive summaries for each of the four consumer groups, with brief encyclopedic intelligence summaries of each of the key industrial, geographic, and civil factors.

STRATEGIC PRODUCTION. Tailored products that focus on establishing *strategic generalizations* pertinent to specific mission areas (e.g. aircraft, automobiles, textiles), specific regions, and specific timeframes (generally long-term).

OPERATIONAL PRODUCTION. Tailored products focused on *regional generalizations* with a special emphasis on industrial areas within the region, on seasonal differences (whether terrain or trade), and on leadership character and demographics.

TACTICAL PRODUCTION.. For each industrial area (or industry area) both generalizations and specifics country by country, with emphasis on terrain, climatic, and civil constraints. It is only at this level that a consumer should have to deal with the level of detail which now characterizes most intelligence community products.

TECHNICAL PRODUCTION. Get away from system-specific production, and move instead toward industry-area production with regional and timeframe sub-sets. Focus on support to cost-benefit and trade-off decisions, not on the system in isolation.

Figure 3B. Model for Consumer-Oriented Production

Four Major Target Groups for Intelligence. There are four specific targets for information and intelligence activities; each of these target groups must be completely understood if a Nation is to maintain both its national security and its national competitiveness. Each target group has a different source of power, and a different way of training, organizing, and equipping itself for battle. Each requires a different intelligence approach and in essence a different kind of intelligence community. The traditional intelligence officer will not be competent against all four of the target sets--four different kinds of intelligence organizations must be trained, equipped, and organized for their specific target set.

a. The High-Tech Brute, similar to the United States of America, is that group which relies on expensive technical capabilities and hugh logistics trains. In industrial terms, this is the capital-intensive player.

b. The Low-Tech Brute, such as the narcotics trafficker or the Italian crime family, represents a "needle in the haystack" problem. In industrial terms, this is the labor-intensive player.

c. The High-Tech Seer, such as highly skilled and knowledgeable computer engineers, is comprised of both conglomerations of skilled individuals engaging in economic warfare, and single individuals, "hackers", able to penetrate advanced computer and telecommunications networks. In idnustrial terms, this is the brain-intensive player.

d. The Low-Tech Seer, such as the Islamic Fundamentalists, or Asian gangs in the United States, are those whose "weapons" are of a cultural or demographic kind, whose "command and control" system is comprised of the television and the pulpit--very difficult for a Western intelligence service to understand and address. In industrial terms, this is the labor union.

In each of these cases, using electronic sources of news and information provides a significant competitive advantage in terms of time, scope of review, and depth of understanding.

High-Tech Brute	High-Tech Seer
High-Tech Brute	Low-Tech Seer

Figure 3C. Four Major Target Groups for Intelligence

Four Kinds of Players in the Open Source Arena. The diagram in the "Background" section clearly identified the nine constituencies in the access arena. Naturally there are sub-constituencies (e.g. government is divided at the federal level into legislative, executive, and judicial, and also into federal, state, and local; media is divided into mainstream national papers, regional papers, niche journals, and technical newsletters).

In general terms, there are four kinds of players:

-- Those who talk to one another but are not influential, are divorced from practical military or commercial applications: the "ivory tower" academics. Spend 10% of your resources on this group.

-- Those who are influential but do not quote one another and contribute nothing substantial: the "bandwagon" journalists. Spend 10% of your resources on this group.

-- Those who are both connected to one another and influential--this constitutes the "mainstream" of current thinking. The downside of the mainstream is that is tends to reflect conventional wisdom rather than innovative or revolutionary thinking. Spend 20% on this group.

-- Those--and they are a small group--that are neither connected nor influential, but who are in fact the "up and coming" leaders in their disciplines. It is this group which not only represents the greatest potential value for a Nation, but which is the least protected! The only obstacle to exploiting this group is internal, it is bureaucratic! Spend 60% on this group. Although intelligence organizations are accustomed to thinking of this group as a source of "sleeper" agents, in fact it should be thought of as a source of "avant garde" thinking which is not only of enormous importance to international competitiveness and domestic security, but predominantly unclassified.

Mainstream (20%)	Up and Coming (60%)
Bandwagon (10%)	Ivory Tower (10%)

Figure 3D. Four Kinds of Players in the Open Source Arena

4. Sources of Information and Methodology

Five Distinguishing Aspects of Information Sources. Sources of information can be classified by medium, location, discipline, language, and level of classification.

The most pervasive medium is hard-copy information. However, most of the hard-copy information is of relatively low grade, and often not worth the expense of acquisition. Never-the-less, it cannot be ignored. Spend 20% of your resources on the hard-copy medium.

The next major medium is micro-fiche; although many organizations are phasing out their micro-fiche holdings, this remains an important medium, particularly in the patent and archival worlds. Spend 10% on this medium.

Electronic information is available through online services as well as offline products. It is important to emphasize that electronic information includes imagery (SPOT, LANDSAT) as well as signals (foreign radio and television broadcasts, unencrypted cellular telephones, facsimiles, and telex transmissions). It is also important to note that, despite the fact that electronic information is a relatively small arena of interest in relation to hard-copy and microfiche, it is "exploding" and already dominates many of the most advanced disciplines as the "medium of choice. For instance, this medium contains over 600 scientific journals online that do not appear in hard-copy at all. *The electronic medium is the battleground where strategic advantage can be gained at relatively low cost and with no political risk--it is open, it is pervasive, and it is not being exploited by other countries as well as it could be--*

this is a very important area. Spend 40% of your resources on this medium.

The most subtle storage medium is the human brain. No intelligence service will ever master the data entry or data collection problem. The most important capability any intelligence service can develop is that of establishing real-time mind-links between the customer and the best available source. The "intelligence minuteman" concept, first articulated in December 1992 at the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", is the wave of the future. Spend 30% of your resources on this medium. Note that this medium provides real-time access to the other mediums--the human expert responsive to tasking can rapidly collect, process, and disseminate essential information from the other mediums, on demand.

It is important to note that in the Age of Information technology has made possible a radical shift in why and when one acquires information. It is now possible to train, equip, and organize collectors of information for "just in time" collection instead of "just in case" collection. Hard copy and microfiche were the dominant storage mediums under the old "just in case" paradigm. Electronic information, and direct access to an enormous global pool of overt human asseets are the dominant access mechanisms under the new paradigm.

The location of the information is both geographic and physical. Some information cannot be obtained without a personal visit to its location. Most information can be obtained remotely, through a telephone call or correspondence, and payment if necessary to the appropriate person.

> *A single researcher skilled at remote data acquisition for a particular region is more valuable than 100 clandestine case officers spread over ten countries. Physicalty the information might be part of a central filing system or a personal filing system. 80% of the time the information will be part of a personal filing system, which reiterates the critical importance of developing human paths to the information.*

Professional disciplines (e.g. physics, electro-optics) are the most global and well-organized structures through which to acquire information. Penetrating a professional association with global links is far more useful than penetrating a single government's nuclear facility, to take one example. Again, professional associations provide the human links and paths toward virtually any information--they are also the most likely to publish information before it becomes classified. It is futile to train intelligence professionals to pretend to be scientists. It is much more useful and cost-effective to provide existing scientists with the finest communication tools and travel budgets possible--they will absorb far more, and be able to report far more, than a few case officers working with a few agents of limited access.

Language skills cannot be ignored. English, French, Spanish, Japanese, Chinese, and Arabic are the most important languages, followed by Russian, Punjabi, Hindu, and Hebrew. Any international intelligence or information service which does not have at least 100 people

fluent in each of the most important languages, and at least 20 people fluent in each of the minor languages listed above, is not serious. Language translation programs (e.g. Global Link) are important aids, and can be used to reduce the time of translation for a typical document from eight hours to three. The importance of linguistic and cultural nuances should not be underestimated. The language of the consumer should be the language of production, even if this involves extraordinary cost.

Level of classification (in governments generally Confidential, Secret, Top Secret, and Codeword; in business generally Proprietary, Trade Secret, Executive Only) is the most misunderstood and over-rated basis for selecting information. Enormous amounts of money are wasted, and significant political risk is undertaken, to obtain information that is classified "secret" or "proprietary". This is a fundamental mistake which reflects a lack of understanding about how knowledge works in society, a lack of understanding of current trends in information sources and methods.

MEDIUM DISCIPLINE CLASSIFICATION

LOCATION LANGUAGE

Figure 4A. Five Distinguishing Aspects of Information Sources

Essential Reorientation of Intelligence Toward Open Sources. The methods used to obtain information should be appropriate to the sector of information generation that is being studied. Each of the nine sectors has information producers. Each nation has representatives of their own in sectors of their own. For instance, your own journalists are frequently the best means of approaching foreign journalists, and of monitoring the production and the human sources being used by foreign journalists.

The fundamental flaw in the "methods" of most intelligence agencies is that they attempt to acquire all information using their own personnel and clandestine or technical methods. Instead, they should leverage the other sectors of the information continuum, and establish a "virtual" intelligence community that is comprehensive. By focusing on open information and the open exploitation of individuals in all sectors, a Nation with a $10 billion intelligence budget can leverage another $90 billion in existing independent but exploitable "virtual" intelligence capabilities whose "overhead" costs are not being paid by the government. The electronic medium is the "lever that can move the world" and give the intelligence professional enormous access.

Privatization of Intelligence

The most fundamental change in "methods", besides moving away from investments in clandestine and technical intelligence capabilities, and toward investments in open source intelligence, is that of the privatization of intelligence. It is more efficient, most cost-effective, indeed, more discreet, to

utilize ad hoc private collectors and processors of information, than it is to use existing bureaucracies, including existing intelligence agencies and existing Embassies or local corporate offices overseas.

Five Elements of a National Knowledge Strategy. This focus on openness is extremely important because it means that the fruits of this open source intelligence effort can be shared directly with industry, the press, and the legislature, without the slightest political risk. For those who do not understand how "open" information can provide a competitive advantage, consider only how disorganized everyone else is--the first Nation to establish a national knowledge strategy which harnesses the full power of their information continuum will achieve an enormous competitive advantage as we enter the Age of Information. A national knowledge strategy is comprised for five elements:

a. CONNECTIVITY. Provide leading representatives within each sector with the telecomputing tools they require to keep in touch with their counterparts in all other countries, and with one another. At the same time, provide government and corporate intelligence analysts with the same tools, and provide everyone with incentives to communicate with one another.

b. CONTENT. Provide incentives to all parties to maximize the amount of information that they put "online"; the government can increase online information by testing new economic models (for instance, the "compound interest" model instead of the "single sale" model for compensating authors) and making appropriate adjustments to copyright and patent law. This is a two-way concept. It is not only important to increase the amount of foreign language material that is captured, translated, and placed online, but it is equally important that great emphasis be placed on exporting national intellectual products which have been fully and accurately translated into major foreign languages such as English, Japanese, and Chinese. In the Age of Information, "gunboat diplomacy" has been replaced by intellectual influence. The quality of a nation's intellectual output, and the degree to which it is made useable by others, will have a dramatic impact on the strategic position of the Nation.

c. CULTURE. Recognize the importance of accelerating the integration of ethnic populations and economically impoverished citizens. In particular, those ethnic groups which speak and read fluently the language of their adopted country, and the language of their former country, are priceless national assets which can be used as interpreters and translators.

d. COIN. A typical major nation wastes on the order of $2 billion a year just on end-user fiddling with personal computer hardware and software combinations. If all redundant and contradictory research & development were brought under control, just in the information technology arena, a typical major nation would probably save on the order of $10-20 billion a year.

e. C4 SECURITY. Every nation, and particularly the advanced nations of Europe

and the Anglo-Saxon world, is extremely vulnerable to the interruption of command & control, communications, and computing services.
Virtually every major antenna system, including the downlinks from the satellites, is completely unprotected. No nation has established a serious C4 security posture that recognized the degree to which government, military, and economic communications depend on a very vulnerable civil infrastructure. No nation has established an effective "cyberspace order of battle". This is the "Pearl Harbor" of the Age of Information, waiting to happen.

CONNECTIVITY CULTURE C4 SECURITY

CONTENT COIN (R&D)

Figure 4B. The Five Elements of a National Knowledge Strategy

5. Industrial Espionage, Sanctions, and Proscribed Information

U.S. Views of Japanese and French. There is a very strong perception within the United States that the Japanese view economic competition as "war", and that the French, while not necessarily viewing economic competition as war, are willing to engage in "unethical" measures including direct support from government intelligence agencies to specific Frnech companies. The book Friendly Spies: How America's Allies are Using Economic Espionage to Steal Our Secrets, while discredited in some circles, has done enormous damage to French interests in the U.S. The running joke about Air France seats being "bugged", very common in U.S. business circles, is a good sign of how deeply this book has penetrated the "psyche" of the U.S. business community.

General Attitudes About Industrial Espionage. Most U.S. companies do not have a full appreciation of how easily others can penetrate their organizaations, and most do not engage in significant industrial espionage. For instance, most U.S. companies have absolutely no computer security and no measures to protect their computers from external penetration. They are completely unaware of the ease with which computer screens and computer emissions can be captured from a van parked outside their building. There is a general sense among U.S. firms that industial espionage is "not worth it". There are two exceptions to this: the first is the hiring of executives and key employees from competitor firms, and the second is bribery, but only overseas.

Sanctions. The Toshiba case is a good example of the sanctions that might be imposed is specific instances when there is a public knowledge of violation, but in general the U.S. government will not publicize or act on cases of industrial espionage.

Proscribed (Prioprietary) Information. There is a strong trend in the United States toward openness. This is true of the government, where many "secrets" and many secret technologies are about to be declassified, and also of industry, where there is a growing understanding that the restriction of information imposes internal costs that may not be

warranted. In the case of specific chemical formulas or other "protectable" secrets, this may not be so, but in the case of general engineering practices, targeted markets, and so on, the general focus is on openness and staying ahead of the competition, rather than on protecting secrets.

6. Analysis

The client is better able to evaluate the applicability of this new theory and practice of intelligence to their needs, but on balance one must conclude:

"Rules of the Game" Have Changed. The Age of Information has redefined our concepts of war and peace, of national security and national competitiveness. The "rules of the game" have changed, and there has been a reordering of both power and the sources of power. Information is now a commodity, and the most important resource to any Nation.

Competitive Advantage Has Shifted From Secrecy to Openness. The Age of Information has destroyed the ability of individuals, organizations, and governments to control information or restrict the dissemination of information. It is virtually impossible to keep a "secret" in this day and age. Hence, the competitive advantage has shifted from those able to conduct research in secret, to those able to RAPIDLY exploit the efforts of others through openly available information collected "just in time".

New "Order of Battle" Needed for National Intelligence. The Age of Information requires a new "order of battle" philosophy within national governments and their major corporate sectors. The degree to which individual minds can be linked across sectors now becomes more important than the number of tanks one has--existing conventional forces can be immobilized, and existing industrial processes can be superceded, by relatively modest applications of knowledge. *The rapid development of competent electronic search & retrieval specialists, and particularly specialists in scientific & technical databases and newsgroups, as well as cultural matters, should be a national priority.*

National Knowledge Strategy is a Critical Initiative. Although there are several nations, including Japan, Sweden, Israel, and Taiwan (and their tribal villages world-wide) which are generally ahead of all others in their national knowledge activities, no nation has actually developed a national knowledge strategy nor harnessed the potential of its nine sectors in the information continuum--a continuum that constitute a "virtual" intelligence community of enormous power.

Strategic Opportunity for Competitive Advantage Exists. A strategic opportunity for competitive advantage exists. In my judgement there is about a two to five year window within which an organized national effort can reap enormous dividends. After that time many organizations will both realize the power of open information and start developing their own collection capabilities more fully, and public encryption will be widespread, introducing a "Tower of Babel" effect into the "electronic English" information commons that is just

beginning to appear.

7. Action Requirements

a. Reinvent National Intelligence. Each nation has an enormous store of non-traditional intelligence and information capabilities outside of government that are rarely called upon. Consider the potential of these non-traditional sources, and develop plans for the total mobilization of the nation's intellectual power.

b. Realign Resources. Roughly 80% of the existing intelligence budget could be realigned to open source intelligence (OSCINT) collection, processing, and dissemination, in close cooperation with the other elements of the national information continuum, who might be inspired to effect their own realignments once they see the government in a leadership role.

CLASSIFIED INTELLIGENCE			**10%**
PROPRIETARY INTELLIGENCE			**10%**
OPEN SOURCE INTELLIGENCE			**80%**
Human Sources		30%	24%
-- "Up and Coming"	60%		24%
-- Mainstream	20%		08%
-- Bandwagon	10%		04%
-- Ivory Tower	10%		04%
Hard Copy		20%	16%
Microfiche		10%	08%
Electronic		40%	32%

NOTE: Column one percentages are 100% of subheading percentage in column two, while column two percentages are 100% of column three subheading. The percentages in column three are actual percentages of the total budget.

Figure 7A. Notional National Intelligence Resource Realignments

c. Establish a National Information Requirements Council. Identify an organization able to coordinate demands for information with global collection activities and impose the common sense guideline of exploiting open sources as "the source of first resort". This has the interesting ramification of also making much more of what we need to know obtainable through private sector capabilities rather than government capabilties.

d. Establish Open Source Focal Points Within United States and Other Countries. Within the United States, contract with two separate organizations: the first should serve as a complement to the Embassy and as a rapid-response local representative for the national intelligence council. It's role should be one of requirements management, oversight, and product packaging. The second organization should actually carry out all the research through sub-contracted collection and production, with value-added quality control. Similar arrangements can be made in other countries, perhaps by building on the established SVP network.

8. References

A resume and a list of selected personal publications are attached. The *Proceedings* of the First International Symposium on "National Security & National Competitiveness: Open Source Solutions", are the sole existing foundation for a national intelligence restructuring of this magnitude. A copy of both volumes is provided as part of this report, together with copies of more recent articles, speeches, and testimony bearing on this issue.

Other works of importance include: Jon Sigurdsom and Yael Tagerud (eds), *The Intelligent Corporation: The Privatization of Intelligence* (Taylor Graham, 1992); Alvin Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (Little, Brown, forthcoming), see especially the chapters on knowledge warriors and the future of the spy. Winn Schwartau, *Information Warfare: How to Wage and Win War in Cyberspace* (Interpact, forthcoming); James Holden-Rhodes, *Sharing the Secrets: Open Source Intelligence and the War on Drugs* (Sandia National Laboratory, forthcoming)

9. Date of Information. 17 September 1993

OPEN SOURCE INTELLIGENCE: PROFESSIONAL HANDBOOK 1.1 Proceedings, 1996 Volume I Fifth International Symposium on Global Security & - Link Page

Previous	Core Open Source References
Next	Concise Directory of Selected International Open Sources & Services

Return to Electronic Index Page