Private Enterprise Intelligence: Its Potential Contribution to National Security

ROBERT DAVID STEELE

LOSING OUR WAY

Too often the intelligence community forgets its roots and abandons its private sector allies. Spies existed before Christ, but most of them were actually legal travelers and discreet merchants. Tea was stolen from China, and porcelain from England, by merchants.1 More recently Japan, China, and Taipei have demonstrated profitable and cost-effective private intelligence capabilities. France and Israel excel at government support to the private sector, but it is possible that soon the private sector will be conducting most of the espionage as well as the open source intelligence (OSCINT) collection for these two countries and many others.

The Western intelligence communities lost their way in the late 1950s, largely because of over-reliance on the American intelligence budget as a safety net, with the unfortunate result that the American tendencies to ignore counter-intelligence and cultural intelligence, and to rely on technical panaceas and bean counting, infected the other services and skewed the manner in which US respective intelligence services trained, equipped, and organized for sustained warfare against ‘the threat’.

Among the worst of the American influences on Western intelligence were its obsessive focus on the Soviet Union as the only enemy worthy of total attention, and an extremely expensive and deceptively ineffective technical collection empire,2 which had the unanticipated impact of precluding American human intelligence (HUMINT) from developing into a serious clandestine service. In the aftermath of World War II the Americans displayed their distressingly usual tendency to take the easy way, and had attempted to penetrate the Soviet Union using enmigrés and others from organizations which had already been thoroughly penetrated by Soviet intelligence. When all of these ‘agents’ were captured and executed, rather than doing some serious soul-searching and then creating a more serious illegals capability, the Americans turned to the U-2 and its follow-on satellites as an ‘acceptable’ alternative to traditional spycraft. Now the US finds itself facing a wide range of threats which are not amenable to technical penetration, while being simultaneously handicapped by the absence of a clandestine service worthy of the name. A side effect of the American dependence upon imagery intelligence (IMINT)

and signals intelligence (SIGINT) overhead collection systems was the abandonment of the robust, diverse, responsive, and relatively inexpensive capabilities of the private sector.

It is instructive, in thinking back to the early days of the Office of Strategic Services (OSS), to consider how very important the academics from the private sector were to the development of our analysis methods, and how very important open sources were to American strategic intelligence efforts. Miles Copeland has described how the OSS handled the innumerable requests from the Department of State and the Pentagon which did not merit clandestine collection. The OSS put two men in a room with The New York Times. Anything that could be answered from this open source was typed up, stamped secret, and disseminated as the purported result of a highly compartmented human intelligence operation – and one which was ostensibly very expensive, hence justifying requests for additional funds. The information itself was not fabricated, only the purported methods of acquiring it.

OSCINT has maintained a modest role within the larger intelligence communities, and a more central role within the smaller intelligence communities, but the reality is that the Anglo-Saxon intelligence communities of today exploit less than 10 per cent of what is available from the private sector. The aim of this essay is to explore the larger strategic context within which private enterprise intelligence can make a contribution to national security; to understand operational concepts from private enterprise intelligence which can and should be adopted by the traditional government intelligence services; and finally, to make an inventory of some of the specific private enterprise intelligence capabilities which can be used by the government to achieve both tactical results and sustained savings.

OSCINT AND THE CHANGING THREAT

Other essays in this collection address the changing threat and changing intelligence agenda, but I wish to outline here an intellectual construct which influenced my early appreciation of how poorly the LS intelligence community exploits private sector intelligence capabilities, and how relevant OSCINT is to the threats that have always been with us, but which are receiving a more appropriate degree of attention today.

While there are obviously variations to these four categories, they helped me focus on the original threat—the high tech brute (conventional military opponent)—while also keeping sight of the three major emerging threat categories. This matrix bears on two fundamental aspects of national security and national intelligence. First, since the National
Security Act of 1947 which created the US intelligence community, all that has followed has led to an intelligence community trained, equipped, and organized to deal with a single monolithic ‘high-tech brute’, the Soviet Union, and very poorly trained, equipped, and organized to deal with smaller high-tech brutes, such as Iraq, or the other three major categories of threat. In particular, national intelligence capabilities in support of both international and domestic law enforcement, and economic competitiveness, are mediocre to non-existent.¹ The US intelligence community does not have the long-term ethnic human penetrations it needs against international criminal or terrorist organizations, nor does it possess the kind of tactical SIGINT capabilities, or even air-breathing tactical IMINT, that would be helpful in coping with these challenging international threats.² Cultural movements baffle ‘Western’ technical indications & warning (I&W) systems because they do not use point to point communications but rely instead on couriers, the pulpit, and broadcast television indirectly to mobilize action elements from within the masses.³ The US does not have an electronic counter-intelligence capability worthy of the name, nor has it established the most basic economic counter-intelligence capabilities.⁴ In short, Our intelligence communities are not ready to deal with three of the four warrior classes⁵.

Second, it is clear that OSCINT can meet the vast majority of America’s intelligence need against the emerging threats, and that OSCINT must be the foundation upon which we completely restructure our classified capabilities. While serving as the senior civilian responsible for the establishment of a new $20 million intelligence production center, the US Marine Corps Intelligence Center, I was shocked to discover that
the $2 million per year earmarked for a Top Secret Sensitive Compartmented Information (TS/SCI) computer system with direct access to data from the Central Intelligence Agency (CIA), National Security Agency (NSA), and Defense Intelligence Agency (DIA) proved to be virtually worthless. The analysts kept coming in saying "there's nothing there but Soviet missile silo data, the Third World "data fill" has not been done." I subsequently discovered that it was possible to meet 80 per cent of the intelligence requirements of the Marine Corps through the use of open sources, at a cost of roughly $20,000 a year expended in subscriptions to LEXIS/NEXIS, EasyNet, Jane's Information Group, and several other private enterprise information services. The private sector is ready now to provide very significant open source intelligence support to the government, and it can serve as a foundation for reinventing and reorienting the clandestine and technical disciplines.

There is a natural tendency on the part of the 'old boys' to say that OSCINT is all well and good, but not for critical national security issues. But senior officers from the US and abroad have said that they are fed up with classified intelligence that is relatively useless to their day to day needs, and are very interested in streamlining and improving their direct access to private enterprise information sources. Two examples highlight needs and shortcomings. First, to paraphrase what was said by the Navy Wing Commander who led the lead flight of 'Desert Storm, against Baghdad:

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

The intelligence community must be mindful of the acceleration of the operational tempo, and of the fact that its consumers are not stupid. They are growing impatient with the inability of the intelligence community to ‘keep up’. In the Gulf War of 1990–91 the classified imagery cycle took eight days from articulation of the requirement to delivery of the imagery. However, the operational planning cycle was three to five days. Classified imagery was not only poorly suited for wide area surveillance, but it was generally too late to be really useful. By contrast, today real-time imagery delivery is available from SPOT, and commercial synoptic one-meter imagery is only a year or two away from reality. Cable News Network (CNN) is blanketing the battlefield, and although it is often wrong, it influences policy and operations. Commercial on-line services and international executive investigative services are offering astute consumers a degree of tailored intelligence support which is not available from the
intelligence community for anyone other than the president or prime minister.

The second example arises from the war on drugs. Los Alamos National laboratory has demonstrated that for $100,000, using only OSCINT, it can do better at estimating global drug production and movement than an equivalent effort by the US national intelligence community at a cost of $12–15 million dollars.

OSCINT AND THE CONSUMER

In considering how best to integrate OSCINT capabilities from the private sector with both old and new classified intelligence capabilities, it is vital to remain acutely conscious of the realities which characterize the consumer's acceptance and exploitation of information. The next figure offers a graphic depiction of the range of 'open sources' reaching the consumer each day, independent of the intelligence community. Ninety per cent of what the consumer reads and listens to is not only unclassified, but also unanalyzed and unrelated to the classified information sent to them. There is no penalty to the consumer for ignoring classified information. Classified information often comes with so much security baggage as to be an untenable contender for the policy-level consumer's attention. Since the executive assistants do not have the codeword clearances, even the consumer's filtering mechanism is of no help in flagging 'useful' codeword material. Finally, unclassified material that fits the consumer's world view or agenda, even if inaccurate, is immediately useful as something which can be disseminated to the press, the public, or parliamentary personalities. The very negative aspect of this chart is that every one of these competing influences has a different agenda, a different world view, a different approach to sources and methods. The policy-maker consumer, in short, is being inundated by babble, and the intelligence community is not helping make sense of it all.

One of the most important changes the intelligence community can make, one which both addresses the potential as well as the hazards of unbridled open sources reaching the consumer directly, is to develop a much more extensive network of analyst-operators assigned to specific consumers and attending directly to their daily needs. Only through day to day interaction, and physical co-location, will such intelligence community representatives be able to: monitor the OSCINT reaching the consumer; earn the consumer's trust and confidence; properly channel requirements for timely action by the classified world; and 'pull' exactly the right intelligence from the classified world in such a way as to be directly pertinent to the consumer's needs of the moment. The second
important change which the intelligence community can make is to redefine itself so that 'the community' is no longer limited to the classified intelligence agencies, but rather encompasses the entire distributed intelligence of the nation, and harnesses the open-source intelligence capabilities of all of these competing influences on the policy-maker.

**OSCINT AND CHANGING DEFINITIONS OF NATIONAL SECURITY**

With the globalization of demographic and ideological movements, crime and the economy, the intelligence community is finding itself hard-pressed to meet the needs of its consumers for intelligence about areas which have traditionally been excluded from its charter. These areas include strategic economic intelligence assessments, which must of necessity draw on comparative domestic economic information, and support to law enforcement in its increasingly dangerous efforts to contain very powerful and ruthless international criminal organizations with solid ethnic cohesion. In this regard, it was instructive to hear Ms Ellen Seidman, Special Assistant to the President of the United States, discuss
her responsibilities on the National Economic Council, and her perceptions of both intelligence and normal governmental information processes. In brief, she found the intelligence community irrelevant to her mandate because in the US the intelligence community is not permitted to develop strategic assessments about domestic matters, including economic competitiveness issues. At the same time, Ms Seidman expressed frustration with the normal governmental information processes, as represented by the Federal Reserve Board and the Departments of Commerce, Treasury, and Labor, because they do not have any concept of how to collect, process, and disseminate intelligence. They did not ‘do’ collection management, or critical analysis, or forecasting, or indications and warning, at the level of sophistication which our intelligence communities have developed over time.18

As intelligence is reinvented, clearly there is a need to reconsider not only sources and methods, but also the range of inquiry and the breadth of the consumer base. The intelligence community must find a new balance between supporting more consumers with non-traditional requirements, including domestic information requirements, while also relying on open sources and private enterprises to fulfill most of the encyclopedic intelligence requirements. The intelligence community, cannot, however, centralize its management of OSCINT, nor can it even presume to control what reaches the consumer. There is a strategic approach which must be taken to integrate government intelligence with private enterprise intelligence.

The Strategic Context of Private Enterprise Intelligence

When we lost our way in the late 1950s, and fell in love with technology and the simplicity of a world with only one ‘main enemy’, we built ourselves a cement bunker with no windows. In their time, satellites were like an oasis in the desert. However, in the past twenty years private enterprise information collection, processing, and dissemination alternatives have exploded – unfortunately, for those within the bunker, with its bad air and depleting supplies, it is difficult to notice such changes.

The strategic context of private enterprise intelligence is a fundamental starting point for the reinvention of intelligence. There is no more promising aspect of the intelligence profession than that offered by the private sector. While we must assuredly pursue improvements in both clandestine and technical collection sources and methods, OSCINT – the private sector – must of necessity serve as both the ‘stopgap’ measure by which we meet requirements for which the community is not trained, equipped, and organized, and also as the benchmark against which we evaluate the value of clandestine and technical capabilities applied to new
targets. At the strategic level, one must consider three points: First, the consumer is now in charge, and acutely conscious of the advantages which OSCINT provides, not only in terms of responsive information at a very low cost, but also in terms of political advantage. OSCINT can be shared with the press and parliament, and therefore is much more politically potent than a secret report which cannot be shared.

Second, this is the age of distributed information. It is simply no longer possible to centralize control over collections, storage, processing, and dissemination. I have stated publicly my view that the ‘Central’ Intelligence Agency is not long for this world – that is not to say that we do not require its capabilities, simply that the way in which it is now organized and managed is so ineffective and inconsistent with the realities of today, that it must disappear.  

Third, it simply is not possible, for both political and financial reasons, to render classified intelligence support to private enterprise with any consistency, or with an assured return on investment. There is no question but that classified economic espionage is required to ‘illuminate the playing field’ for the government policy maker. However, given the fragmentation of ownership, management, and employment of most international firms, defining a strictly American or strictly Canadian firm meriting the expenditure of taxpayer funds for classified intelligence becomes problematical. I believe that the single best thing the government can do for national competitiveness is to nurture the growth of what Lee Felsenstein calls the ‘information commons’ of open source multimedia data. For example, Keith Hall the Deputy Assistant Secretary of Defense for Intelligence and Security has stated clearly that while intelligence must of necessity rely on OSCINT for context, intelligence is intended to collect secrets not available ‘by other means’, and that OSCINT falls firmly within the category of ‘other means’. This poses a dilemma. On the one hand, the intelligence community should continue to focus on secrets. On the other hand it is essential to keep the policymaker informed, and 80 per cent of the time OSCINT is better at informing policy than is secret intelligence. The US needs a new strategic definition of what constitutes ‘national intelligence’, a definition which provides for a distinction between classified government intelligence and unclassified private enterprise intelligence, while also providing for the integration of both under the national intelligence umbrella. The isolation of the intelligence community from its consumers, and the arrogance of the community in presuming that it knows best who its consumers should be, and that it knows best whether secrets are better than open sources in any given instance, must be brought to an end.

In essence, it is not enough for the government simply to understand
and take advantage of private enterprise intelligence. It is essential that the government have a national information strategy, and that it nurture distributed centers of excellence. It is not enough to expect that the private sector will undertake the necessary collection and processing that is required – government must actively encourage such endeavors, without controlling them, and constantly monitor the state of its national information continuum. Figure 3 illustrates the 'information continuum'. It is very important to note that the intelligence community is but one ninth of that continuum, and that existing security and procurement practices assure the complete isolation of the intelligence community from the other eight sectors. If one regards the intelligence community as the pinnacle of the national information continuum, then the most interesting aspect of reinvention is that associated with new responsibilities for the community – nurturing distributed networks which are unwitting or benignly witting, and most assuredly not 'under control'.

What I call the 'information continuum' is the knowledge terrain within which government intelligence and corporate intelligence must operate:

**FIGURE 3**

THE 'INFORMATION CONTINUUM' OR 'VIRTUAL INTELLIGENCE COMMUNITY'

<table>
<thead>
<tr>
<th>Schools</th>
<th>Private Investigators</th>
</tr>
</thead>
<tbody>
<tr>
<td>K-12</td>
<td>Libraries</td>
</tr>
<tr>
<td></td>
<td>Information Brokers</td>
</tr>
<tr>
<td>Universities</td>
<td>Business</td>
</tr>
<tr>
<td></td>
<td>Media</td>
</tr>
<tr>
<td></td>
<td>Defense</td>
</tr>
</tbody>
</table>

The continuum consists of elementary and secondary schools, universities, libraries, all businesses and their information repositories, private investigators and information brokers, the media including the trade journal and scientific and technical media, governments down to the state and local level, all defense and law enforcement organizations, and the official and usually secret intelligence communities. *If we can harness this distributed power, then we can create a 'virtual intelligence community' far more capable than the isolated communities now in existence.*

The good news is that this continuum provides a low-cost, flexible, and responsive 'virtual research department' of extraordinary power and value. The bad news is that very few people know how to navigate this terrain, or how to break down the barriers between sectors, industries, and individuals. In order to bridge the gap between what exists in the 'real' intelligence community today, and what might exist in the 'virtual' intelligence community of tomorrow, a national information strategy is an essential pre-requisite. Whether through legislation or through administrative fiat, there must be a concerted effort by government to
harness the 'distributed intelligence of the nation'. In addition to the connectivity that comes with the National Information Infrastructure (NII) and its international extension, the Global Information Infrastructure (GII), three other elements are required to fully harness private enterprise intelligence. First, since most private enterprises, be they commercial or academic, simply will not trust the intelligence community to 'manage' or 'control' their databases or their activities, the best way to harness the distributed power of the private sector is to create a National Information Foundation (NIF), which is non-regulatory and distributes funds (rather than centralizes information) to 'centers of excellence' chosen because of their focus on specific regions or topics of interest to the government. The NIF might be modeled after the National Science Foundation, which nurtures distributed centers of excellence without attempting to control them or their content.

Second, expenditures for information research and development (both tools and content) must be coordinated to avoid duplicative or counter-productive investments. Third, communications and computing security must be assured through national standards, testing and certification laboratories, due diligence legislation, and national education.22

In brief then, while the private sector provides a very robust foundation for reinventing intelligence, and private enterprise intelligence can today be exploited well beyond what the intelligence community is doing, only a national program and a national strategy which explicitly recognizes the distributed nature of private enterprise intelligence, and seeks to harness it, will yield the optimal value for national security and national competitiveness. The intelligence community cannot harness the distributed intelligence of the nation. Only the people and their government of the whole can reinvent intelligence.

*Operational Concepts, Policies, and Practices*23

At the operational level, which deals with top-level guidance of overall intelligence efforts, rather than the specific research tasks common to the tactical level, the focus should be on some core concepts where the private sector is ahead of the intelligence community.

- **DECISION SUPPORT** is the only acceptable mission for intelligence. One must carefully distinguish between *data*, which is the raw text, image, or signal; *information*, which is collated data of generic interest, such as newspapers or research reports; and *intelligence*, which is information that has been tailored to support a specific decision by a specific person about a specific topic at a specific time and place.24
• COLLECTING SECRETS is not difficult if you focus on collecting them before they become secrets. The weakest link, and the cheapest and easiest to exploit, is the grey literature and human infrastructure responsible for doing research just before someone decides to label something proprietary or classified.  

• CAST A WIDE NET. For example, do not make the same mistake as the French steel industry. It worked very hard at competitor intelligence against other steel industries, and completely overlooked the plastics industry, which was busy developing steel substitutes.  

• OPENNESS VERSUS SECRECY. The openness paradigm has won. The example of the nuclear industry, based on secrecy and not very progressive, is instructive when compared with the openness of the electronics industry, where competing engineers compare their approaches over coffee.  

• JUST IN TIME VERSUS JUST IN CASE. Paul Evan Peters, Executive Director of the Coalition for Networked Information, makes the point that in the age of distributed information easily accessible through electronic connectivity, it makes no sense to store volumes of out-of-date information when you can reach out and get exactly what you need in the way of current information on a 'just in time' basis.  

• LEVERAGE EVERYONE ELSE’S OVERHEAD. An expansion of the above concept is that of avoiding the enormous costs of attempting to maintain, with limited sustainability, in-house experts and in-house archives on everything. The private sector contains many superb information and intelligence capabilities where the resident expertise, and the existing databases, are maintained at someone else’s expense. The intelligence community must do a much better job of exploiting such centers of excellence. The most important contribution these external elements can make is not as a substitute for in-house analysis and the final production of an integrated classified product, but rather as self-sustaining information filters and on-demand experts able to rapidly identify the latest and best multi-media information pertinent to a specific decision area – information that can then be rapidly acquired, evaluated, and integrated into the all-source product. Dr Joseph Nye (former Chair of the National Intelligence Council) described the intelligence problem as a jigsaw puzzle, with open sources providing the outer edge pieces (context), without which one can neither begin nor complete the puzzle.
• DIAMOND VERSUS LINEAR PARADIGM. The old paradigm for information acquisition is the linear model, where the consumer goes to the analyst who goes to the collector who goes to the source, and then back up the chain the answer goes. This paradigm is not only too slow, it is not workable when you have a fast-moving topic with lots of nuances that are difficult to communicate to intermediaries. The new paradigm is the diamond paradigm, where the consumer talks to the analyst, the collector, and on many occasions the source, in order to ensure there is a timely and accurate meeting of the right minds.

• CIO: CORPORATE INTELLIGENCE OFFICER. The last person corporations should appoint to the CIO position is the oldest informations systems expert. They are technicians and do not have a complete understanding of corporate strategy and the needs of senior executives for real-time content displayed in meaningful ways. The CIO position should not only be responsible for ensuring that the entire corporation – every employee – serves as part of the collection network, but also for ensuring that the information in hand is exploited, and that the corporation has the broadest possible network of external collection and processing capabilities on demand. The CIO should be the intelligence community’s primary point of contact for legitimately and openly unclassified information.

• INFORMATION VALUE: CONTENT + CONTEXT + TIME. Corporations and banks have a wealth of information that is rotting away unused rather than being bartered or made available to one another as a means of increasing the competitiveness of an industry or a country. If one understands that stripping information of time and context allows it to be bartered without losing a competitive advantage, while gaining additional information in the process, then the way is open to operational-level agreements which will increase an individual firms competitiveness as part of a larger consortium. The intelligence community should be the catalyst for a national program to inventory existing information that is in storage or available through private enterprise collection networks, and then devising means of accelerating the transfer of basic information to the information commons.

• INFORMATION-DRIVEN ACTIONS are better than mission-driven actions. Many corporations as well as government organizations appear to be mired in old organizational practices where a business unit is given a specific series of tasks to accomplish, and is then expected to accomplish those tasks over and over again
without reference to the external environment or other elements of the corporation.

- **CORPORATE HIVE.** Every employee is a collector, producer, and consumer of intelligence. Drivers of delivery vehicles, service technicians, those responsible for cold calls on customers, all should receive special training in observation and elicitation, and should have easy to use channels and processes for reporting what they see and hear. The concept of ‘national hive’ merits pursuit."

In brief, then, we must think of each organization within the information continuum as an information network, with each citizen-employee being in turn responsible for exploiting those external information networks that they come in contact with – quite literally, *everyone* becomes a collector and producer of intelligence.

**CONCLUSION**

*In the information age, '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, in order to provide 'just in time' decision-support to the consumer.*

In a period of rapidly changing and emerging threats, when fiscal resources for national intelligence are in decline, open sources are proving to be far more capable and responsive than any intelligence analyst would ever have expected, and cost a fraction of their classified counterpart disciplines. The private sector is a nation’s first line of defense, and also its first line for collection and processing. It is the private sector which offers the cheapest and fastest indications and warning, current intelligence, and estimate intelligence capabilities.

The concept of ‘central’ intelligence simply will not survive. ‘National intelligence’ must be redefined, and the intelligence community reinvented, in order to harness the distributed intelligence of the nation, while permitting the intelligence community to conserve its scarce resources. *The intelligence community must focus on satisfying a broader range of consumers, on outsourcing and exploiting open source intelligence collection and analysis to the maximum extent possible, and on developing clandestine and technical collection capabilities that are truly discreet and able to achieve results without exposure.*

National intelligence communities cannot remain isolated entities relying solely on classified in-house capabilities funded by the tax-payer at great expense. Without a national information strategy, and national
vehicles for harnessing the distributed private enterprise intelligence capabilities of the nation (and of other nations), national intelligence communities are at risk of both a 50 per cent cut in their budgets (or worse), and relegation to an obscure role as special action teams restricted to in extremis tasking. The bottom line, however, remains the consumer of intelligence. Today’s consumer is sophisticated and constantly exposed to the wide variety of private enterprise intelligence capabilities. Today’s consumer is also beset by fiscal constraints, and it will not take the consumer long to realize that there may be some advantages to ‘raiding’ the intelligence community’s budget in order to ‘distribute’ intelligence resources among the consumers themselves. If the intelligence community does not master OSCINT and provide the consumer with a ‘value-added’ contribution in relation to OSCINT then the day is going to come when the consumer will testify to parliament that they do not read classified intelligence, they do not want classified intelligence, and they are not willing to pay for classified intelligence. On that day, intelligence as we know it will die.

It is our burden and our privilege to work together to ensure that from the ashes arises a new form of national intelligence, a national intelligence which fully integrates and harnesses the distributed capabilities of each nation, and serves as the foundation for national security and national competitiveness. Together, in combination, the unclassified capabilities of private enterprise intelligence and those of classified government intelligence can form a ‘virtual intelligence community’ without equal, a virtual intelligence community able simultaneously to inform policymakers, the business community, the academy, and citizens.

NOTES

1. The privatization of intelligence is a concept – indeed a sub-discipline – which owes a great deal to Dr Stevan Dedijer of Lund University in Sweden. His contributions were honored with a book dedicated to him, by Jon Sigurdson and Yael Tagerud, The Intelligent Corporation: The Privatization of Intelligence (Taylor Graham, 1992). More recently, aided by one of his doctoral student-lecturers, Ms. Katarina Svensson, PhL, he published Technical Attachés and Sweden’s Innovation Intelligence (Lund Univ., April 1994). See also, Loch K. Johnson, ‘Seven Sins of Strategic Intelligence’, World Affairs 1462 (Fall, 1993); and his subsequent book, A Season of Inquiry: The Senate Intelligence Investigation (Lexington, KY: UP of Kentucky, 1985).

2. Although the technical disciplines, both imagery and signals, have much to offer intelligence communities, the reality is that they process less than 10 per cent of what they collect, and disseminate roughly 10 per cent of what they process (ergo they disseminate 1 per cent of what they collect). Thus, it is highly questionable as to whether the technical disciplines provide the return on investment that they should, in comparison with either clandestine intelligence or open source intelligence. Detailed comments on the costs of secrecy are contained in Testimony and Comments on Executive Order 12336,

4. Miles Copeland, *Without Cloak or Dagger: The Truth About the New Espionage* (Simon & Schuster, 1974), pp.47–8. Four recently retired KGB officers, speaking at an Open Source Solutions 1993 conference on the topic of ‘Soviet Exploitation of US Open Sources During the Cold War,’ described how often ‘Centre’ would ‘catch them in the act of using open sources as a substitute for successful agent operations, and how open sources were in fact a mainstay of their Cold War scientific and technical collection efforts. The officers speaking were all colonels: Vladimir B. Barkovskiy, (former Deputy Director, KGB Science and Technology Inst.); Yuri I. Molin, (former Deputy Director, Research Inst. on Intelli. Problems); Vsevolod I. Gapon, (former Deputy Chief of Division, KGB); and Yuri H. Totrov, (former KGB Section Chief for Counterintelligence, Central Intell. Agency Affairs).


7. When the author participated in reviews of intelligence effectiveness against low intensity conflict targets, one of the most critical deficiencies was the fact that US systems could not deal with ‘low slow singleton’ targets. A major deficiency within the military is its propensity to procure ‘fast movers’ (jets) with very limited later times over the target area, while declining to invest in the necessary ‘sensor to shooter’ collection and connectivity, so that these expensive aircraft can be effective against LIC targets.


11. The Foreign Broadcast Information Service (FBIS) and the excellent scientific & technical intelligence capabilities developed by the National Air Intelligence Center (NAIC), the National Maritime Intelligence Center (NMIC), and the National Ground Intelligence Center (NGIC) all merit respect. Unfortunately, the US intelligence community spends less than 1 per cent of its budget on open sources, while admitting that open sources provide 40 per cent of the all-source product. By the author’s estimate it is tapping less than 10 per cent of the private sector’s capabilities. Among the obstacles to improved OSCINT are an archaic security system, a culture that thrives on secrecy.
rather than results, and a procurement system that makes it very easy to spend millions on hardware, while making it virtually impossible to subscribe to LEXIS/NEXIS or pay a consultant a quick $1,000.

12. One Marine Corps general has stated that he used to talk about intelligence being broken, until he realized that this implied it existed. In his view, national intelligence simply does not ‘exist’ when it comes to supporting expeditionary military operations.


15. James Holden-Rhodes, SHARING THE SECRETS: Open Source Intelligence and the War on Drugs (forthcoming), extract from Ch. 5.

16. This chart is reproduced from Steele, 'A Critical Evaluation', Fig. 11, p. 98, and in turn was taken from the CIA 'Intelligence Successes and Failures Course', which has been discontinued.

17. See Andrew Shepard, 'Intelligence Analysis in the Year 2002: A Concept of Operations', paper presented at the Symposium on Advanced Information Processing and Analysis, Reston, Virginia, 24-26 March 1992. Mr Shepard articulates how on-site intelligence analysts can fulfill three major roles in direct support of the consumer: real-time validation and review of OSCINT reaching the consumer independent of the intelligence community; real-time retrieval from intelligence community databases of that information which can be tailored to support an imminent decision by the consumer; and collection management tailored to the needs of the consumer rather than the circumstances of the collectors.

18. Ms Seidman was speaking to the Open Source Intelligence Lunch Club in Washington, DC on 11 Jan. 1994. Her remarks were reported in OSS Notices Issue 94-001, 21 Feb. 1994, p. 10.

19. My most detailed statement on where I see the US intelligence community developing, to include the dissolution of the CIA (and the establishment of a separate Clandestine Services Agency) is contained in 'Policy and Practice', OSS Notices 2/6 (3 Aug. 1994), pp. 2-4. Among the highlights: dissolution of the CIA; establishment of a separate Clandestine Services Agency (CSA) under total non-official cover; conversion of the Directorate of Intelligence into the cadre for an inter-agency series of intelligence centers under the oversight of the National Intelligence Council; creation of Deputy Directors of Classified Intelligence for Research and Development, and for Communications and Computing; integration of the National Reconnaissance Office (NRO) with the Defense Mapping Agency (DMA) to create a Defense Mapping and Reconnaissance Agency which contracts out 75% of its collection and production; expansion of the National Security Agency (NSA) charter to include monitoring of unencrypted cyberspace data and the establishment of a clandestine capability for inserting alternative transmitters into sites using unbreakable encryption; and expansion of the Defense Intelligence Agency (DIA) to manage a totally integrated Intelligence Corps which provides the military intelligence personnel to all military elements from the forward-most tactical element through the Joint Intelligence Centers (JIC) and into the Pentagon.

20. Lee Felsenstein works at the Interval Research Corp. in Palo Alto, California. Interval represents an attempt to create a modern Xerox Parc.

21. See 'Remarks of Mr. Keith Hall, Open Source Lunch Club', OSS Notices 2/6, pp. 8-9.

22. Absolute private security is an essential pre-condition to complete openness. In order to engender the kind of open exchanges that are needed in a distributed intelligence system, it is essential that individuals feel that they: know who is on the other end with
some certainty; will receive the original document without modification; and can rely
on a digital cash payment being transferred if that is part of the exchange.

23. The operational concepts outlined here represent a revised version of Robert D. Steele,
'Access: Theory and Practice of Competitor Intelligence', *Journals of the AGSI* (July
1994). The article reprints the author's keynote address to the Assoc. for Global
Strategic Info. (AGSI) meeting in Heidelberg, Germany, 14 June 1994.


25. For a detailed articulation of my theory and practice of OSCINT, see Robert D. Steele,
'Access: Theory and Practice of Intelligence in the Age of Information', in *Proceedings
of the Second International Symposium on 'National Security and National Competitive-

26. Herve Serieux, Vice President of the Inst. for European Leadership, as included in his
address to the French information industry congress, IDT '93, in Paris during June
1993.

27. John Perry Barlow, 'Remarks', in *Proceedings First International Symposium: Open


29. See Kevin Kelly, *Out of Control: The Rise of New-Biological Civilization* (Addison-
Wesley, 1994), note 20.