

***Notes for a Presentation to
OSS '03***

***Greg Fyffe
Executive Director, Intelligence Assessment Secretariat
Privy Council Office, Ottawa, Canada***

"Intelligence Sharing and OSINT"

I am speaking this afternoon as the head of a government assessment organization. Government analysts find it useful to attend discussions like this to explore the potential for open source exploitation, to learn more about technological innovations, but also to hear prominent experts with different perspectives on world events.

My expertise is not on OSINT, but on the work environment of analysts.

A year and a half ago I spoke to this meeting on "A Canadian Perspective on Global Coverage". I put forward a number of ideas that I won't go back over in any detail, but which are related to my comments today.

First, we need to remember that most assessment services are small, and their needs and relationship to OSINT are different than those which apply to the United States.

Second, there are many mental maps around which we can organize our intellectual view of the world. Recognizing these maps—globalization, democratization, terrorism, ecological change, and the role of the US—is part of self-conscious analysis.

We try to be aware of the value of mental maps in generating insights, but not impose limitations on our vision of possible future developments by mistaking those maps for a comprehensive view of reality.

Finally I suggested some things that the OSINT community could look at in partnering with the intelligence community—providing regular updates and summaries on important on-going crises, tracking the cumulative impact of cross-boundary issues such as ecological change or global crime, providing a forum for the debate of ideas, and a forum for debating globally important questions. I was not suggesting none of things exist,

just that they were potentially useful tools for the intelligence community that could be enhanced by OSINT partners.

Robert suggested that I speak on the general issue of intelligence sharing, and the central question for this group—to what extent can open source sharing promote inter-national and inter-agency intelligence sharing. My principal point, if you don't mind my giving it away at the start, is that formal intelligence sharing at the inter-country level is governed by very well understood rules, and these rules are necessary for the intelligence community. The parallel OSINT community will sometimes want to shadow these rules, and sometimes it will want to add value by breaking completely free of their constraints.

Intelligence agencies all accept that a large portion of the material they must collect, understand and assess comes from open sources.

The proportion is usually cited as between 85 and 95%;

Open source exploitation is accepted as a central method of research by all agencies I am familiar with, although to what degree the full potential has been reached is not something I can evaluate.

The remaining 5 to 15% of intelligence that is covert rather than OSINT is the principal source of intelligence that relates to important aspects of capability, a high portion of intent, and almost all valuable counter-intelligence information. When we move from context to specific threat the relative value of open source versus covert reverses.

Intelligence sharing includes sharing assessments, and trading views at the formal and informal level.

The most comfortable sharing arrangements evolved during and then after the Second World War. Sharing between the United States and the United Kingdom has been far-reaching, and these two countries are the core of formal arrangements which include Australia, Canada, and sometimes New Zealand. These countries have evolved bilateral relationships with many other countries. Some of these relationships, such as between the United States and Germany, have been very important.

These relationships remain extremely important, but the overall context of intelligence sharing is not static. The terrorist threat, and the end of the

Cold War, has shifted some of the intelligence war from country versus country, or alliance versus alliance, to many countries versus terrorist groups. The web of relationships is complex, a spread-out alliance of close friends, pretty close friends, sometime associates, and very temporary, partial allies, who still no doubt devote most of their resources to spying on each other.

Before coming back to the implications of some of these new relationships, let's look at the nature of the most formal sharing arrangements.

There are very precise implicit and explicit criteria around intelligence sharing which govern whether a relationship exists and the depth it develops.

First, intelligence links develop between countries because they have common values. This seeds an expectation that sharing will advance these values and benefit the national objectives of the countries involved.

Second, there is a common sense of threat, or a common target definition. Allies have enemies in common and assume that dividing lines between friends and enemies are very long term. Intelligence sharing complements common diplomatic objectives and integrated military preparations.

Third, intelligence sharing is facilitated by a common spoken language. This may seem trivial, but it takes time and significant expense to translate a piece of intelligence or an assessment, and nuance in some circumstances is all. Language is one of the reasons the US, UK, Australia and Canada are natural partners, although Canada is bilingual in its internal conversations. Language differences do not prevent alliances, but they can encumber them to a degree that frustrates comprehensive sharing, where it would otherwise be desirable.

Fourth, a fundamental principle of sharing is give/get—the more an intelligence partner puts on the table, the more it can take from the table.

Fifth, sharing countries must have confidence in the security arrangements of intelligence partners. Sharing at very high levels of security means knowledge of how material was collected, and even at lower levels a knowledge of what was collected. Depending on the nature of the relationship, material can be sanitized to the appropriate level of

sensitivity. Even assessment sharing at the Confidential level, with the removal of sensitive information, can be beneficial for comparing perspectives, conclusions and predictions.

Sixth, sharing involves an understanding of its limits. This is governed by all of the other considerations, particularly give/get, common objectives and mutual confidence. Equally, even close allies have different national interests and therefore limits to sharing.

Finally, as a seventh criteria, agencies can only share what is theirs. Information is controlled by the originating agency and cannot be put into the basket by a receiving country for sharing with a third country outside the sharing partnership.

These criteria lead to different levels of sharing. Countries can share perspectives and conclusions, then detailed assessments, and finally highly classified analytical pieces. They may share raw or processed intelligence which lies behind the analysis, and specific intelligence reports. In the closest cooperative arrangements, countries can share information on sources and methods, specific collection resources, or they may jointly undertake collection or security operations.

Intelligence sharing may take place along several scales, from very limited discussion on a particular case, to a high degree of regular institutionalized interaction in the long term, best illustrated by the relationship between agencies in the United States and the United Kingdom, as noted earlier.

Sharing is extensive and for partners is invaluable, but there are practical limitations which restrict some of the benefits, in particular for analysts.

Accurate assessment is prey to unchallenged assumptions, mirror imaging, inadequate collection or intellectual blindness, and so partner agencies like to test their analysis against that of analysts with a different cultural, national or agency perspective.

Sharing material is easier than debating assessments in detail. Analysts from different countries do trade perspectives, but neither have the time, nor the technical means, to do this on a regular basis. There are practical and theoretical objections to such things as inter-partner chat rooms that are currently not surmountable.

Much of this gap is filled by inter-agency visits, classified colloquiums, and the activities of liaison officers who attend briefings, pose questions, participate in discussions, and report back to their home agency.

Formal country-to-country sharing is extensive and highly beneficial, but it does have natural limits governed by the demands of work and broad diplomatic considerations.

OSINT has some specific advantages to contribute to intelligence sharing.

The OSINT community is infinitely varied and can be as broadly defined as we wish. Intelligence agencies, by comparison are more homogenous, and face challenges when they try not to be.

OSINT discussions or forums are not linked to domestic foreign policy and there is a capacity to be inclusive not open to intel agencies.

OSINT can easily go outside the usual community.

OSINT practitioners, because they are so numerous and because of the way they work, build up extensive contact networks, reaching into the business and NGO worlds.

If the on-going sharing of views between partners is highly desirable, and if open source advocates believe they have a role to play, what can they add? Is it more information? Is it more reliable prediction? Is it greater insight, or greater knowledge of sources? Is it the capacity to generate debate and discussion?

One important opportunity for the OSINT community would be to promote a definition of the intelligence community which is broader than the formal alliances.

Formal alliances take a long time to build, are linked directly to extensive diplomatic cooperation, and depend on complex understandings around security practices and intelligence targets. OSINT organizations can include non-traditional actors, recognizing for example, that China is a key partner in dealing with the DPRK, and a number of non-allied nations are partners against terrorism.

Including non-traditional partners in on-line or in-person forums would bring a wider sharing of perspectives. It goes without saying, which is why I am saying it, that this would have to be facilitated with some care. There is a comfort level even in OSINT in holding discussions among people who are consistently on the same side.

OSINT conferences have more flexibility than government agencies in deciding who to invite. Organizers can assemble the combination of experts that they feel would produce an enlightening conversation. Intelligence analysts benefit from the range of views, and the chance to meet colleagues close and distant to react to the presentations. This can promote discussion on issues which may be unorthodox, politically incorrect or, we would hope, unusually prescient.

Intelligence is preoccupied with future developments or intentions and possibilities, as well as with current issues of capability. The future is a mystery, but at least its unclassified.

OSINT-based forums can debate some of these mysteries, especially those where covert material is of marginal use. One of the issues constantly facing analysts, and which both Carmen Medina and Stephen Ward comment on their articles "What To Do When Traditional Models Fail," and "Evolution Beats Revolution in Analysis," is how far we can go in making predictions that go beyond the evidence. Analysts need to offer useful predictions to readers, but there is still a limited tolerance for serious error. Can we debate some of these issues with the professional futurists, who spend their careers trying to find ways of being insightful about the future?

The professional intelligence community has increasingly turned to diverse bodies of experts to probe the future. But perhaps OSINT can range wider and push the boundaries. Perhaps many in the intelligence community would welcome this.

There is also a role for OSINT shocking those of us trying to understand the contemporary world. In common with most of humanity I find it more pleasant to talk to someone who agrees with me than someone who considers most of what I believe to be foolish and naive. We don't pay much attention to people who challenge the orthodoxy of free markets, universal human values, free speech, or the right of civilized people to live in peace.

Unfortunately, the great cataclysmic shocks of the twentieth century were orchestrated by fanatics (communists, fascists or anarchists) who believed in none of these things, and managed to persuade millions of others that they shouldn't believe in them either.

We should listen to the distastefully unorthodox even if we must listen with scepticism and hostility. How are we to avoid mirror imaging unless we know the extreme difference between other perceptions and our own?

After the bombing of UN Headquarters in Baghdad the CBC newscast had a panel of experts speculating on the forces behind it. One hinted that the US itself had reasons for attacking the UN in Iraq.

The panelists dismissed the suggestion with contempt, but the question for me was not whether this silliness might be true, but how anyone could believe something so illogical and remote from any connection to evidence or basic reasoning. As we know from some of the reactions to 911, there are commentators, not just in the Arab world, who advanced theories that seem not just silly but mad.

I don't suggest we should invite crazies, but we should be prepared to see our frames of reference and world view challenged so that our analysis is resilient.

OSINT is about exploiting information, but of course the purpose of intelligence, open or covert, is insight. What does it all mean? Why are things happening the way they are?

One of the most persistent reasons for intelligence sharing is the search for another valid perspective, another explanation for the facts, factors hidden from our particular field of vision, but fully in the open for another?

OSINT forums which ask "why?" as often as "what?" "where?" and "how?" will provide value to the professional intelligence community and promote a broader discussion.

My own experience is that intelligence analysts are interested in very broad questions about the future of humanity and the planet, but don't

have enough time to debate the issues with people who spend their lives pursuing those questions.

It would be useful to see a more direct connection, via OSINT, between the mega-theorists and intelligence analysts.

I began with a discussion of the principal written and unwritten rules behind intelligence alliances—common values, a shared diplomatic agenda, mutual confidence on security, give/get, don't share what isn't yours.

These rules are vital to national intelligence sharing. OSINT doesn't have to be bound by any of them.

Some OSINT forums will promote sharing by alliance partners if they do parallel and follow those rules, reinforcing the formal covert communities with informal open source ones.

The value of other OSINT forums could be exactly the extent to which those rules are discarded and consciously reversed.

OSS '03 BEYOND OSINT: Creating the Global Multi-Cultural Intelligence Web Proceedings Supplement Holiday Inn Westpark Rosslyn Washington, D.C. 15-19 September 2003 - Link Page

[Previous](#) [OSS '03 Brian Czech The Stead State Revolution for National Security and International Stability \(Slides\),](#)

[Next](#) [OSS '03 Jim Hardee Special Operations OSINT,](#)

[Return to Electronic Index Page](#)