



UNIVERSITY  
OF WOLLONGONG  
AUSTRALIA

University of Wollongong  
Research Online

---

Faculty of Arts - Papers (Archive)

Faculty of Law, Humanities and the Arts

---

2006

# Publicly shared intelligence

G. de Valk

*University of Amsterdam, The Netherlands*

Brian Martin

*University of Wollongong, [bmartin@uow.edu.au](mailto:bmartin@uow.edu.au)*

---

## Publication Details

de Valk, G & Martin, B, Publicly shared intelligence, *First Monday: Peer-Reviewed Journal on the Internet*, 2006, 11(9). The original article is available [here](#).

Research Online is the open access institutional repository for the University of Wollongong. For further information contact the UOW Library:  
[research-pubs@uow.edu.au](mailto:research-pubs@uow.edu.au)

## Publicly shared intelligence

by Gilliam de Valk  
and Brian Martin

## Abstract

Publicly shared intelligence is the gathering and analysis of information of political value that is openly available to the public and able to be tested. This is a potential alternative to the sort of secret intelligence normally carried out by government agencies. Desirable features of publicly shared intelligence can be determined by analogy to other open knowledge production systems, including science and open source software. The case of the Shipping Research Bureau illustrates the potential of publicly shared intelligence. We outline features of a publicly shared intelligence system, including implications for public education.

## Contents

Introduction

Open knowledge systems

The Shipping Research Bureau

Towards publicly shared intelligence

## Introduction

Intelligence services have a mixed record. They can cite some memorable successes, especially in war-time espionage and code-breaking, but there are also some spectacular failures. These include failure by U.S. agencies to prevent the attacks of September 11 and the assessment, prior to 2003, that Iraq had weapons of mass destruction. Especially in the last case there is a debate about how much responsibility lies with political leaders rather than intelligence services to create so-called stovepipes (Hersh, 2003).

Because so much about the intelligence process is secret — including problems caused by secrecy itself (CIA, 1977) — it is difficult to make an accurate assessment of the typical quality of intelligence. Significant information about the track record of intelligence services has been made publicly available in only a few countries. It is extremely difficult to assess the success rate of agencies, because of two opposite processes. First, successes will be often kept secret to protect the *modus operandi* and information position of the agency. Second, agencies may have an interest in promoting their successes and hiding their failures.

There are several responses to shortcomings of intelligence services. One is to give them more power and money, as occurred in the U.S. after the intelligence failure of September 11. Another is to seek reform, as occurred in the U.S. through legislative controls after the abuses of the 1960s were exposed, though such reforms may be resisted or reversed (Olmsted,

1996). A radical solution is to abolish an agency altogether, the fate of the Foreign Intelligence Service in the Netherlands in 1994. But this too has risks. There are threats to communities for which early warning and advanced preparation are invaluable.

Here we examine a different approach that differs greatly from the traditional intelligence community. We question two conventional assumptions about intelligence services, namely that they must operate largely in secret and that they must be run by governments. By questioning these assumptions, we are led to the idea of intelligence services that operate openly — at least in terms of their conclusions — and are run as independent enterprises. We call this alternative publicly shared intelligence or PSI. It involves public testing of intelligence [1].

National intelligence services do not operate in total isolation. Many of them share intelligence with each other, including sometimes with ostensible opponents, on the basis of shared interests, for example in relation to arms control treaties. There is also a quite limited sharing of information with outside groups, including non-government organisations such as Amnesty International. But this level of sharing occurs within operating procedures in which secrecy is central.

Outside the conventional intelligence sector, there are some organisations and initiatives that include elements of publicly shared intelligence. For example, Statewatch (<http://www.statewatch.org/>) collects and publishes considerable information on European developments in civil liberties, policing, surveillance, refugees, prisons, racism and security. Statewatch uses open sources and investigative efforts to collect information on state threats to civil liberties.

Other groups in this category include Privacy International, American Civil Liberties Union (ACLU), Electronic Privacy Information Center (EPIC), Center for Defense Information, Federation of American Scientists, and human rights groups and groups that monitor sales of weapons to repressive regimes, such as Amnesty International, Safer World and Campaign Against the Arms Trade.

In the next section, we briefly discuss other open knowledge systems in order to extract principles or lessons that can be useful for understanding what PSI might look like. Then we take a close look at one prototype of PSI, the Shipping Research Bureau, with an eye for what distinguishes it from conventional intelligence. In the concluding section we give a tentative outline of features of PSI, mentioning relevant examples and ideas for introducing this alternative.



---

## Open knowledge systems

The most well known system of open knowledge production is scientific research. A key element of science is its openness. Robert Merton, the founder of the sociology of science, said that science was, or should be, characterised by four norms: universalism, communism, disinterestedness and organised scepticism (Merton, 1973). The norm of communism, later renamed communalism, required that scientists share their findings with each other. Similarly, prominent scientist and science policy analyst John Ziman (1968) characterised science as “public knowledge,” the title of one of his books.

Scientific publications operate as the currency of scientific research. In them, scientists reveal not only their findings but also their methods. Scientific facts, formulas and theories are publicly available and can be used freely by other scientists for their own investigations, with

acknowledgement through citations the only expected return. Scientists engage in research for their own intellectual satisfaction, for the practical benefits that result and, not least, for peer recognition that is manifest through citations, invitations to conferences, and awards. Competition for recognition for scientific contributions that openly build on each other has, arguably, been responsible for the incredible dynamism of science. Another important factor has been ample funding.

In the ideal operation of science, some things remain confidential. What actually happens in the laboratory is not usually public knowledge; only the formal record, in the form of a publication, is open, and this typically misrepresents the messy process of research. Peer reviewers are normally anonymous. This can lead to abuses such as rejection of a competitor's contribution, but the existence of large numbers of scientific journals means that publication is seldom prevented but only delayed. Note that considerable training is often required to understand research findings: scientific knowledge may be open but for non-specialists it might as well be in code.

Science in practice often deviates from the ideal of openness. Quite a lot of research, notably military and commercial research, is undertaken in secrecy. Intellectual property puts constraints on the use of some research techniques. The quest for recognition leads many scientists to hide key parts of their research from competitors. In addition, funding and conflicts of interest can lead to biased findings; important areas may be neglected because research interest is influenced by funding, often tied to commercial or government priorities. These problems are recognised by many scientists and policy-makers, who deplore the way that secrecy and vested interests can restrain scientific progress.



**... scientific knowledge  
may be open but for  
non-specialists it might  
as well be in code.**



Despite its shortcomings, science is an exemplar of the advantages of an open knowledge system. The keys to science's dynamism seem to be publication of research findings and the incentive that scientists have to build on these findings, in a system of competition for peer recognition and potential application of results, with ample funding. The existence of multiple publication outlets overcomes, eventually, most problems due to review by anonymous peers. Some of the greatest perceived threats to science come from secrecy and control over knowledge linked to government and corporate vested interests.

Another important open knowledge system is open source software (Moody, 2002). The basic idea is that software is developed through a process of public peer contribution. Typically, an individual or small group writes a first draft of code for a particular purpose, which is made publicly available for comment. Anyone can point out problems or suggest modifications to improve efficiency or eliminate bugs. A core group — which might be an individual — receives these comments and decides what changes to make in the code, and also decides when the code is ready for release.

Some open source software is released under a GNU licence, which makes it publicly available but prevents anyone from copyrighting it. The licence allows others to make modifications to the software, thus enabling a process of continual improvement as well as tailoring versions for specific purposes. The most well-known open source software is the operating system Linux, which is widely used and admired for its stability.

The advantage of open source development process is that software is scrutinised by numerous skilled practitioners, often from diverse viewpoints, leading to a robust product. In the classic open source model, all contributors are volunteers: they assist for their own satisfaction and for their pride in helping create a quality product that is socially useful. In contrast, proprietary software during its development is usually scrutinised by a smaller and more homogeneous group, due to a need to maintain secrecy. Because proprietary software is created by salaried workers (in an environment where efficiency and costs take priority) there can be problems resulting from premature release, self-interest, career building, and sometimes worker resentment that can lead to sabotage.

The open aspects of open source software development are the software itself, the suggested modifications and the general process by which it is written. The revision process, carried out by the core group, is not usually open. Note that writing of high quality code requires a certain level of expertise; few non-programmers have any idea what this involves.

Open source software development has several similarities to scientific research; indeed it can even be conceived as part of science (Kelty, 2001). Both aim at producing a form of knowledge through a process of open peer review, in which outputs can be used as a basis to make improved versions. Any competent practitioner can contribute. Exclusion occurs by the level of expertise required and through self-selecting core groups. Parts of the process of producing knowledge — namely, the details of producing and revising work — remain out of sight, but the final results are openly available.

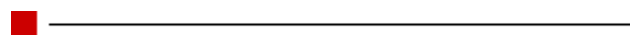
There are also some differences between scientific research and open source software development. Most scientists are full-time professionals, whereas most open source contributors are volunteers. The scientific enterprise receives vast funding and is a key part of educational systems whereas open source has grown out of an ongoing social movement, namely the free software movement. Open source is closer to early science carried out by amateurs. Commercialisation of open source approaches possibly may lead to greater similarities to modern science.

Based on this brief examination of science and open source software, three key elements of open knowledge systems seem to be knowledge in the public domain, peer review, and an opportunity for anyone to contribute.

Another development in open knowledge systems is wikipedia and other wiki and related systems. They rely on openness and voluntary contributions from knowledgeable members of the public (Stalder and Hirsh, 2002). So revolutionary are the possibilities of open knowledge production created by distributed networks that it is possible to speak of a new mode of production, governance and property based on the dynamic of peer to peer (Bauwens, 2005).

Conventional intelligence is almost the opposite of open source knowledge. Conventional intelligence is prepared in secrecy and is not peer tested except in-house. And often this in-house review is seriously limited by the need-to-know principle. Failures are often hidden and hence repeated. The uses of intelligence are restricted to those with official access, often extremely limited.

PSI thus would be a dramatic contrast to conventional intelligence. We now turn to an example of PSI in action: the Shipping Research Bureau.



## **The Shipping Research Bureau**

In the 1980s, the Shipping Research Bureau (SRB or the Bureau) monitored oil shipments to the apartheid regime of South Africa. The Bureau published its research findings in reports, surveys, and newsletters. It was founded in July 1980 by its parent organisations Holland Committee on Southern Africa (HCSA) and Kairos, two Dutch mainstream anti-apartheid organisations. The SRB was a small foundation with only one to four staff members. Various governments and other groups financed the Bureau, including Sweden, Norway, the United Nations, trade unions and churches. In fourteen years, the total budget of the Bureau was less than US\$2 million. As a comparison, the wide variety of sanctions increased the estimated cost to South Africa for obtaining oil in the 1980s by more than US\$2 billion *per year*.

The overall goal of the SRB was to contribute to a wider implementation of oil embargoes against the apartheid regime of South Africa. In the view of the Bureau, this could be reached through a trio of embargo politics — legislation, monitoring and enforcement [2]. The SRB wrote “Publicity and Action are Effective” (SRB, 1990). The Bureau is likely to have been the only private agency in Dutch history that had a powerful lobby in Parliament to promote its reports and its political aims. By its role through the United Nations, the SRB also was a major player in this field on an international level, being seen as the “most active non-governmental organization” helping to achieve an effective oil embargo against South Africa [3].

In its reports and surveys, the SRB presented the general features of its methodology. Yet, details remained *de facto* secret. In its publications, it gave information on the four stages to prepare a report — the initial gathering of data, findings submitted to companies for corrections, findings submitted to governments for investigation, and the final analysis and decisions about the findings.

Databases by Lloyd’s were the main initial source for the SRB to investigate ships that had supplied South Africa with oil. Lloyd’s was not mentioned by name in SRB reports, which just said, “[t]he Bureau’s main sources of data regarding these ships have been specialised shipping industry publications and computerised data bases.” [4] Though the SRB used a different reporting format than Lloyd’s, insiders in the world of shipping companies could readily infer the importance of Lloyd’s databases for the SRB. But the Bureau also had dozens of other sources.

After 1988, the research design changed fundamentally and investigations became much easier. The SRB then obtained direct access to sources within South Africa with accurate data on the actual delivery of oil. Earlier, it could trace 50–60 percent of the estimated shipments; after 1988, this rose to 85 percent.

The Bureau had to deal with manipulated data. Actually, several parties employed a policy of deception, trying to frustrate the SRB’s investigations. For example, ship owners stopped calling at Lloyd’s, made fake calls at other harbours, and kept the chartering of tankers secret. South Africa made special laws and took measures to enforce the secrecy of oil supplies. In South Africa, ships started to call under coded names or there was radio silence. Another popular method was to paint over or to cover the ship’s name when unloading at Durban or Cape Town. All kinds of other methods were conceived. Informants purposely fed the SRB disinformation. At some point, the Bureau was even infiltrated by another private agency.

If the Bureau discovered a deception, it could undertake three types of additional activities: extra internal assessment, development of new sources, and employment of new research methods. Deception led to the mobilisation of new resources and an improved information flow that in the end led to analyses of a higher quality than if no deception was found. Such effects are not uncommon, and are — in an analogous way — described by Wilensky when he says that only urgent and crucial policy decisions can activate high-quality intelligence,

because of the necessity to communicate out of normal channels [5]. Deception seems to trigger off some of the effects described by Wilensky.

The Shipping Research Bureau worked in a highly politicised environment. For a good understanding of the consequences of this, we first present some information on peer review and on the forum function caused by the open publication of reports.

At the Bureau, peer review and forums for feedback and criticism were well developed. Internally, there was a well-established forum in which the method of peer review — and ways to supplement and to refine this method — was discussed with the help of two external advisors. Also internally, peer review helped to tackle decisions on the publication of difficult cases of oil supplies. Externally, a lot of feedback was created by the publications themselves, by reactions from governments, oil and shipping companies, and media. What seems to have been decisive for a positive effect on the quality in the SRB case is a combination of different forums from different backgrounds.

Yet, not all the effects of the feedback forums were straightforwardly positive. The publication of reports led to an extra bias in reports during a couple of years. In the first main report by the Bureau, some OAPEC (Organisation of Arab Petroleum Exporting Countries) countries were accused of delivering oil to South Africa. These countries had endorsed an oil embargo. The SRB and the South African ANC had agreed earlier the ANC could make itself familiar with the raw material of the pre-publication findings. Because of protest by its political allies, the OAPEC countries — through, for example, the U.N. Special Committee against Apartheid — and the ANC put pressure on the Bureau. For the second report, the ANC and the SRB agreed “the research findings would be presented in a manner as to ‘avoid the impression’ of blaming the oil-producing countries primarily and to ‘stress the responsibility of companies.’” [6] After protests by oil transporting countries, companies, media, and others, in 1985 the SRB abandoned this policy of veiled and biased reporting.

Such diplomatic pressures are capable of seriously harming the quality of a report. A negative diplomatic influence can also be traced at the U.N. In 1986, the U.N. established the Intergovernmental Group to Monitor the Supply and Shipping of Oil and Petroleum Products to South Africa (U.N. IGG). The U.N. IGG made use of documents handed over by governments. Although the U.N. IGG was aware these documents were sometimes forged, for diplomatic reasons it did not put these falsifications aside. The U.N. IGG deleted cases even when a party involved admitted delivering oil to South Africa.

The negative effect of diplomatic and political pressures also affects public agencies. In the case of the assessments by U.S. and U.K. agencies on Iraqi weapons of mass destruction, it is likely these pressures played a major role. Diplomatic and political pressures are the only plausible explanation for the differences between assessments by these agencies and statements made by a series of UNSCOM and UNMOVIC officials, such as Hans Blix, Rolf Ekéus, Scott Ritter, and the Dutchmen Jan Rozing and Cees Wolterbeek (Zembla, 2004).

Two experiences of the SRB case are of relevance for the development of PSI (de Valk, 2005). First, a policy of deception by opponents — as to manipulate or to hide information — does not necessarily lead to a lower quality of the intelligence reports. Instead, deception can trigger extra activities and hence may actually raise the quality of a report.


A second issue concerns peer review and feedback by third parties. Obtaining feedback — including peer review — is important for raising the quality of a report. A presumption here is that the agency in question is willing to evaluate the feedback in an objective and distanced way. Yet, one form of feedback has a destructive potential: diplomatic pressure. Succumbing to this sort of pressure will hurt an agency’s public credibility and influence.

This leads to the observation that openness is connected with more than one feedback

mechanism. The positive effect of openness is undoubtedly that it creates external forums. A negative effect is that it may trigger additional diplomatic pressure.

In the SRB case, the power of the external forum turned out in the long run to be stronger than the power of diplomatic pressure. The positive effects finally dominated totally. Here, the openness eventually had a complete self-cleansing potential.

In some cases, though, diplomatic pressure may be stronger than the external forum. In that case, a self-cleansing potential of a different nature will be established — those who do not adjust their report will lose their credibility and influence.



**... there is a need for a  
*triangulation of forums*  
composed of *different*  
backgrounds. This is  
likely to be a more  
decisive factor than  
openness *per se*.**

.....

The worst situation seems to be if an agency has only one diplomatic or politically motivated forum, either an internal or an external one. The risk of bias will then be greatest. The implication is that there is a need for a *triangulation of forums* composed of *different* backgrounds. This is likely to be a more decisive factor than openness *per se*.

In the struggle for good intelligence, traditional agencies suffer a double handicap. First, their forum function is seriously compromised by the secret nature of their work. Second, what is left of this eviscerated forum is often for a considerable part composed of political and diplomatic feedback and pressures. These political and diplomatic pressures are precisely the ones that have a serious destructive potential on the quality of their intelligence.

A final remark on the SRB case: source protection was hardly an issue in relation with reports being made public. The Bureau had some vulnerable sources, including deep throats in the shipping industry and even from within South Africa. But source protection did not stop the SRB from publishing its reports, nor did it interfere with the external forums with their positive effect on quality. The SRB case indicates that source protection is not an automatic excuse for a lack of openness of reports.



---

## **Towards publicly shared intelligence**

Having looked at the features of successful open knowledge systems, especially science and open source software, and at a successful example of PSI, the Shipping Research Bureau, we now present some ideas about what a more developed system of PSI might look like.

The first and most obvious feature of such a system is that the findings of publicly shared intelligence bureaux (PSIBs) would be publicly available for scrutiny. This might include assessments of foreign political developments, economic analyses, examinations of weapons systems, assessments of trade in dangerous goods, risk analyses of technological



developments, and inside reports on organisations. It would also include explanations of how intelligence is gathered, but probably not information on precisely who provided which bits of data and not necessarily who offered internal peer review of findings, namely review carried out within PSIBs.

The second feature of the system is that findings of PSIBs would be subject to external peer review. If a PSIB consistently made mistakes or failed to forecast important developments, it would lose credibility, whereas PSIBs with track records of accuracy and foresight would gain credibility. Reviewers of PSIBs could establish rating systems for clients; reviewers would themselves be open to peer review.

A third feature is that there would be many different PSIBs. Some might cover specialised areas and serve a small clientele but others would cover a range of areas for a broader audience, in competition with each other. No PSIB would have a guaranteed monopoly, thereby reducing the risk of corruption.


PSIBs might be run as commercial enterprises, as non-profits relying on grants, or as entirely volunteer operations. Independence of funding agencies is important for the credibility of PSIBs, but there are different ways to achieve this. One method is to obtain support from multiple independent funding agencies, so that the PSIB is not dependent on a single source. Others are to have an endowment or rely on public subscriptions.

It is easy to raise objections. For example, PSIBs might become the target of sophisticated operations to flood them with misleading information. But that is no different than what happens with current agencies; there is no reason why openness should be a disadvantage for dealing with the challenge. Another objection is that by publishing its findings, an PSIB would jeopardise the potential for secret investigations and stings. But this is not so different from what happens today with the news media.

Rather than debate the pluses and minuses of PSIBs in the abstract, a more pragmatic approach is to set some up, with ample funding, and see how well they operate. This would be a process of social experimentation, analogous to scientific experiments with peer review of findings. Given the level of rhetoric today about the wonders of markets, it is striking that most intelligence services continue to be funded and run by governments, often as monopolies. PSI should be seen not just as a matter of bureaux but as a part of a wider social process that might be called social intelligence. To be effective, competent intelligence provision must be matched by competent users or consumers: those who make use of intelligence findings need to understand the strengths and limitations of the information they receive and to understand the capacities of the agencies that provide it. With PSI the capacity of users is doubly important, because they are both users of intelligence and contributors.

Conventional intelligence makes use of information provided by the public, but in a very one-sided fashion. To use a familiar example, police services usually welcome tip-offs from the public, sometimes putting out appeals for information about suspects. But this is mostly a one-way process, with little feedback from the police to the public except through news reports of prominent investigations and prosecutions. Police services usually make only limited efforts to inform the public about the sorts of information that they would like to receive, and there is no systematic training in skills for helping police.

PSI depends much more on a supportive public. Hence there would be a need for popular education, through the media, formal classes and study circles, in areas such as understanding threats, collecting information in daily life, operating cameras and computers, and effective communication. The best way to develop PSI is by going ahead and developing PSIBs that serve useful functions. If intelligence is produced by totally different types of organizations (conventional and PSIBs) competition eventually will lead to a higher quality of their

products and more accountability. 

## About the authors

Giliam de Valk recently completed his PhD at Rijksuniversiteit Groningen, the Netherlands, and now teaches intelligence studies at the University of Amsterdam and the University of Utrecht. Brian Martin works in the School of Social Sciences, Media and Communication, University of Wollongong, Australia, researching nonviolent action, dissent and other topics.

## Acknowledgements

We thank for Jochen Gläser, Robert David Steele and Steve Wright for comments on drafts of this article.

## Notes

1. A different alternative to secret intelligence is open source intelligence (OSINT). The most prominent advocate of OSINT is Robert David Steele (2000, 2002; <http://www.oss.net>), who sees it as part of a complete rethinking on intelligence. Steele (2002, p. 164) defines OSINT as “unclassified information that has been deliberately discovered, discriminated, distilled and disseminated to a select audience in order to address a specific question.” For policy-makers, OSINT has the great advantage that it does not need to be kept secret: it can be used in discussions and negotiations.

Steele envisages OSINT being produced by a variety of organisations, both government and private. A key open source is the Internet, but there are others such as Russian military maps. Producing OSINT requires far more than a search of the Internet: it involves advanced skills in information gathering and synthesis as well as understanding what is important to the client. Steele sees OSINT as cost-effective compared to secret intelligence, but believes the two are complementary.

Although OSINT is gathered from public sources, the resulting intelligence is not necessarily open itself. It might be provided, for example, by a private corporation to a government agency. It is not secret in sense of being classified, but it may be available only to the producer and client and not freely available to others. As will be seen, PSI and OSINT differ in a number of regards.

2. Hengeveld and Rodenburg, 1995, p. 175.

3. SRB, 1993/94, p. 2.

4. SRB, 1990, p. 95.

5. Wilensky, 1967, pp. 81, 84.

6. Hengeveld and Rodenburg, 1995, p. 98.

## References

Michel Bauwens, 2005. "The political economy of peer production," *1000 Days of Theory* (1 December).

CIA, 1977. "Critique of the codeword compartment in the CIA," at <http://www.fas.org/sgp/othergov/codeword.html>, accessed 6 April 2006.

Giliam de Valk, 2005. "Dutch intelligence — Towards a qualitative framework for analysis," PhD dissertation, Reijksuniversiteit Groningen.

Richard Hengeveld and Jaap Rodenburg (editors), 1995. *Embargo: Apartheid's oil secrets revealed*. Amsterdam: Amsterdam University Press.

Seymour M. Hersh, 2003. "The Stovepipe," *New Yorker* (27 October).

Christopher M. Kelty, 2001. "Free Software/Free Science," *First Monday*, volume 6, number 12 (December), at [http://www.firstmonday.org/issues/issue6\\_12/kelty/](http://www.firstmonday.org/issues/issue6_12/kelty/), accessed 3 April 2006.

Robert K. Merton, 1973. *The sociology of science: Theoretical and empirical investigations*. Chicago: University of Chicago Press..

Glyn Moody, 2002. *Rebel code: Linux and the open source revolution*. Cambridge, Mass.: Perseus.

Kathryn S. Olmsted, 1996. *Challenging the secret government: The post-Watergate investigations of the CIA and FBI*. Chapel Hill: University of North Carolina Press.

Shipping Research Bureau, 1993/94. "Newsletter on the Oil Embargo against South Africa," number 33, fourth quarter 1993/first quarter 1994 (speech of Anthony Nyakyi, chairman of the U.N. Intergovernmental Group to Monitor the Supply and Shipping of Oil and Petroleum Products to South Africa).

Shipping Research Bureau, 1990. *Fuel for apartheid: Oil supplies to South Africa*. Amsterdam: SRB.

Felix Stalder and Jesse Hirsh, 2002. "Open Source Intelligence," *First Monday*, volume 7, number 6 (June), at [http://firstmonday.org/issues/issue7\\_6/stalder/](http://firstmonday.org/issues/issue7_6/stalder/), accessed 3 April 2006.

Robert David Steele, 2002. *The new craft of intelligence: Personal, public, and political*. Oakton, Va.: OSS International Press.

Robert David Steele, 2000. *On intelligence: Spies and secrecy in an open world*. Oakton, Va.: OSS International Press.

Harold L. Wilensky, 1967. *Organizational intelligence: Knowledge and policy in government and industry*. New York: Basic Books.

Zembla, 2004. "De waarheid van de wapeninspecteurs," *NPS/VARA*, broadcast of 15 April, at <http://redir.vara.nl/tv/zembla/welcome2.html?archieff>, accessed 24 August 2006.

J.M. Ziman, 1968. *Public knowledge: An essay concerning the social dimension of science*. Cambridge: Cambridge University Press.

## Editorial history

Paper received 5 April 2006; accepted 10 July 2006.

---

[Contents](#) [Index](#)



This work is licensed under a [Creative Commons Public Domain License](#).

Publicly shared intelligence by Giliam de Valk and Brian Martin  
*First Monday*, volume 11, number 9 (September 2006),  
URL: [http://firstmonday.org/issues/issue11\\_9/valk/index.html](http://firstmonday.org/issues/issue11_9/valk/index.html)