The RUSI Journal
Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/rusi20

Open source intelligence

Stevyn Gibson

Version of record first published: 11 Jun 2008.

To cite this article: Stevyn Gibson (2004): Open source intelligence, The RUSI Journal, 149:1, 16-22

To link to this article: http://dx.doi.org/10.1080/03071840408522977

RUSI

Open Source Intelligence

An Intelligence Lifeline

Stevyn Gibson

Stevyn Gibson is currently undertaking PhD research into 'OSINT and the National Intelligence Machinery' at the Department of Defence Management and Security Analysis, Royal Military College of Science, Cranfield University. This article was awarded First Prize in the RUSI Trench Gascoigne Prize Essay Competition 2003

Lord Hutton's comprehensive verdict in favour of the government and against the BBC (read media generally) was delivered on 28 January 2004. A leading Law Lord, Hutton gave his 'ruling' in a judicial fashion: he found in favour of one of the two sides implicated in the Inquiry into Dr David Kelly's death. Although critics have challenged the one-sidedness of his report, its findings were based on an exhaustive review of evidence led by an eminent jurist with a reputation for integrity and independence. That said, a central question that has dominated the national debate since Dr Kelly's death – whether pre-war intelligence informed government decision-making or *was formed* to support decision-making – was not addressed in the Inquiry. Its omission fuelled calls for a new independent inquiry, which was duly announced by Prime Minister Blair on 3 February. Expected to report by summer 2004, this new inquiry will investigate the accuracy, validity and reliability of the pre-war intelligence product, particularly concerning Iraq's WMD threat but perhaps also the former regime's alleged links to Al-Qa'ida.

Until then, the public will be none the wiser about the challenges of the intelligence process and no clearer on the traditionally stated and acceptable role of intelligence: to inform decision-making – independently, impartially and with integrity. Hopefully, this article, written before the Hutton Inquiry was published and unchanged since, may go some way to clarify that.

Introduction

The September 2003 Hutton Inquiry represents a low point in the standing and *raison d'être* of the UK national security intelligence function. The low point both reflects and obscures the key question from which this Inquiry has emanated: has intelligence, with respect to WMD and links to Al-Qa'ida, been pushed or pulled in order to derive a *casus belli*? More broadly put – is intelligence used to inform decision and policy-making or is intelligence formed to support their pre-determination? The perception in the public mind ranges from confusion to boredom, while the worrying conclusion being drawn by many eminent scholars of intelligence seems to be coalescing around the latter view, that intelligence is being selected and harvested to prop up pre-determined policy.[1] If this is the case, then intelligence, both product and process, will be tainted as a result.

However, still greater forces are at work – reflections of contemporary society that are even more capable of overwhelming the intelligence function than Hutton. This article attempts to throw intelligence a lifeline by examining the emerging role of open source intelligence (OSINT), drawing together the contextual influences that are bringing about its potentially starring role and identifying the contribution it can make to defence and security in return.

Forces of change

Emerging from the Hutton Inquiry are equally encouraging signs that demonstrate a desire for openness in civil society generally and in the intelligence community in particular. The very public nature of the inquiry, the unprecedented scrutiny of key intelligence and security service officials, and the dissection of the intelligence process at its highest levels, all demonstrate an acquiescence, if not willingness and determination, to bring intelligence out of the closet.[2] Nevertheless, not wishing to diminish the

The intelligence function can reform and adapt to all three shapers of global, postmodern, risk society or react to maintain the status quo and become irrelevant in the process

benefits for national corporate governance that Hutton is having, the verdict at the Royal Courts of Justice will not be sufficient to preserve intelligence, informing or formed, from new forces at work in contemporary society.

Three such forces seem pre-eminent. First, the framework in which much of civil society is conducted, not just in developed nations but also globally, has changed irreversibly to the context of 'postmodernism'. Second, taken-for-granted concepts of the nation-state, democracy, trust and freedom are under threat from the activity of globalization in its free-market, consumer-oriented form, which nation-state governments seem unwilling or unable to protect themselves against.[3] Third, the ubiquitous phenomenon of risk is the new altar at which all decision and policy-makers must now worship. The intelligence function can reform and adapt to all three shapers of global, postmodern, risk society or react to maintain the status quo and become irrelevant in the process. Rathmell acknowledges this dilemma when he discusses the need for a 'postmodern intelligence' responsive to these forces of change.[4]

Postmodernism

Postmodernism is largely a developed-nation phenomenon but with global consequence. It is the culmination in the evolution of Western societies from hunter-gatherer through settled agriculturalist, the Enlightenment, industrial revolution and the information-technology communication age to the contemporary world in which we live.[5] Its characteristics include:

- The end of industrialization and the era of information processing into knowledge as the single most significant portion of the service sector;
- The end of mass production and the recognition of the individual together with the consequent creation of niche markets;
- The globalization of commerce and economics;
- The ease of travel and collapse of borders;
- The explosion of information and information overload; and
- The emergence of the citizen with rights, aspirations, education and influence.[6]

Postmodernist themes are dominated by growing realizations that:

- There is no grand formula for life rather a continual process of dealing with combined complexity, uncertainty and ambiguity;
- Objective evidential science is no longer enough. Rather, social and cultural constructs of how the world 'is', also play their part.[7]
- Sciences, disciplines and philosophies are blurring, sharing and learning from each other;
- The spread of knowledge is transforming hierarchies and centralized bureaucracies into networked individual centres of excellence; and
- A growing recognition that everything is connected to everything else.

During the course of the last fifteen years – with the collapse of the Soviet Union, the removal of the Cold War's bi-polarizing world influence, the more recent 9/11 terrorist attack (as much an attack on the perceived ends of globalization as on America), the combined 'paradise' of liberal democracy and moral consciousness that Europe luxuriates in, the pre-emptive power displays that the US dips in and out of as it chooses to move between world policeman and isolationist state[8] – the world has transitioned from the modern to the postmodern.[9] The ramifications for many, certainly in most of the developed world, is that life has become more complex, fast, interdependent and uncertain than it has ever been. Equally, postmodernism is creating a world dominated by risk to such a degree that its management (particularly where the risk is negative) has become almost mandatory, for individuals, organizations and societies alike, to undertake.[10] Postmodernism travels under many pseudonymous, from Ulrich Beck's 'risk society' to Slovic's 'post normal science' to Fukuyama's 'posthuman future'. They all particularly note the change in the conduct and order of civil society effected by science's spin-off - technology.[11]

Globalization – democracy, trust and freedom

The end of the Cold War dragged us out of a torpid, linear and polarized historical cul-de-sac and propelled us back into history's more customary but turbulent flow. Yet postmodernism is not only characterized by the collapse of

The issue for OSINT is no longer its validity or usefulness but rather how could it be developed, institutionalized and rolled out as a discipline common to government intelligence analysts and commercial knowledge workers alike

communism, the release of tribalism and the emergence of catastrophic terrorism but also by globalization's impact upon the 'nation-state' and its attendant mainstays of democracy, trust and freedom.[12]

The very globalization that brings much in the way of progress is also the rallying point against which 'collective-Jihad' is waged, not only by Islamist religious extremists but also by a range of the dissatisfied, disenchanted and disenfranchised. These range from 'anti-globalizers' to 'countryside-alliancers', across multi-national, multi-religious and multi-class groupings, curiously united against centralizing governments and, as Barber describes them, 'McWorld' type corporations, as they see not progress but only threats to their way of life.[13] Therefore, it is no longer just the nation-state that requires an intelligence function, which until recent times has been exclusively delivered by the public sector, but also the corporate world, and for that both are turning to OSINT particularly when the public sector appears reticent or unable to assist.[14]

Confucius said: 'without trust we cannot stand.'[15] In any given society, democracy survives because trust in all its institutional manifestations is firmly rooted in the people and culture of that society. From the loyal opposition to the apathetic but 'content' voter, democracy is embraced. Democracies break down because that trust is not deep-rooted enough – geographically, socially, culturally and temporally – to survive 'difficult' times such as occurred in Germany's post-First World War Great Depression or the USSR satellite states of the late 1980s.[16] Trust occurs across a rainbow of relationships from inter-personal to international. Key contributors to the establishment of trust at any level, whether between you and your neighbour or between nation and nation, are openness, co-operation, communication and the personal nature of its giving and receiving. The intelligence function within a democratic society enjoys a two-way relationship with the public it serves. The public trusts it and it creates trust in the collective mind of the public. The currency of exchange is information, in the broadest sense of the word. If that currency is restricted then trust diminishes with it.

Risk – complexity, uncertainty and ambiguity

Risk is measured by the product of its constituents: likelihood (p) and impact (I). If only risk were that simple! From SARS to Sadaam we live in a complex world. However, complexity is now too simple a description of today's world. The promise of unlimited progress, offered by human intervention through science and technology at the dawn of the industrial revolution, now brings fear and detriment in equal measure at the end of it. Renn elucidates a catch-all taxonomy that characterizes postmodern risk as predominantly complex, uncertain or ambiguous.[17]

Complex risk can be managed to a considerable degree by the application of science and technology, then driving them (such as those presented by nuclear power in the early 1970s) towards acceptable levels. Complexity is not the problem. Uncertainty and ambiguity, present to varying degrees in each and every risk alongside complexity, bring additional challenges to risk management that can contradict and negate the work of scientists. Ambiguity and uncertainty are a growing feature of postmodern society. Ambiguity is science's political equivalent of 'debate'. There is little scientific argument about the data, the methodology or the observation, but considerable disagreement about what all this measurement means. The polarized scientific debate over GMOs is proving a classic example.[18] Nanotechnology is already on the horizon! Uncertainty is manifest where scientific regulation struggles to play catch-up with the very scientific development that it is supposed to be regulating. Uncertainty is not just ambiguity's inability to quantify or qualify impact but additionally the incapacity to scientifically measure likelihood. Terrorist risk displays both – immeasurable likelihood and unimaginable impact.

Thus risk has a 'dual nature', characterized by risk theoreticians as a combination of its objective reality and its social construct. Scientists can manage the objective nature but its social construct demands repeated reassurance from people who can deliver valid messages – risk managers, whether they are regulators, government or private bodies – that they are not only endeavouring to assess and treat risks but also identify them, communicating and disseminating what they find. A critical step in this process is the creation of knowledge to inform social construct. Knowledge that can be communicated and disseminated freely is a small but valuable part of the response to the changing force of complex, ambiguous and uncertain risk.

Finally for risk – it is managed not solved. Risk management is a process not an objective. Managed risks leave behind residual risks, which are re-examined or accepted until such time as science or other methods catch up and deal with them. In the intervening period society

should be educated to accept and live with those risks by becoming habituated to them rather than irrationally expecting them to be removed instantly.[19]

Open Source Intelligence (OSINT)

OSINT is the analytical exploitation of information that is legally available and in the public domain.[20] That is to say it is neither acquired clandestinely through espionage or illegal means nor 'closed' to the public by government or commercial sensitivity. Such information has always been available but the last two decades have given it a recognition and usage commensurate with many changing aspects of contemporary society as both a product of it and a tool to deal with it.

OSINT need not necessarily be obtained openly in that the acquirer leaves a calling card. It can be discretely acquired. Information, obtained clandestinely or openly, whose disclosure creates vulnerabilities for sources, methods or intentions, must of course become 'closed' by classification or commercial sensitivity procedures. However, classification without justification, preventing communication and dissemination rather negates the potential of OSINT. Regrettably, 'need to know' has become a debate complicated more by issues of organizational culture and personal vested interest than operational security. The mounting dilemmas of global, postmodern, risk society and the recognition of the value of OSINT, of themselves, are creating pressures to change this. However, a reactionary intelligence community wishing to preserve all that is 'traditional' will only compound and reinforce these dilemmas.

What sources are there? The Internet, and before that newspaper 'cut-and-paste', are no longer the stereotypes of OSINT. Indeed the Internet is not of itself a source but merely the means by which sources are accessed. Open sources can broadly be categorized into: traditional media broadcast such as that captured by the BBC Monitoring Service or Foreign Broadcast Monitoring Service (FBIS); commercial 'on-line premium' such as Factiva, Lexis-Nexis or Dialog for global media coverage; specialist technical/tactical coverage such as Jane's, Oxford Analytica or the Economist Intelligence Unit; 'grey literature' – information which is obtained from expert channels including academia and private information brokers; overt human observers – the most valuable means of ascertaining 'ground truth' such as International Alert and Amnesty International; commercial imagery – there are some eleven private (commercial) high-resolution (near 1m) remote sensing satellites available to credit card holders;[21] and mapping specialists such as Eastview Cartographic, suppliers to the US DoD for Afghanistan, Iraq and most recently Iran(!).[22] It is worth noting that in all of these categories a significant and critical issue implicit to each of them, and one that remains to be addressed by OSINT as well as intelligence generally, is the issue of language. We ignore at our peril Steele's estimate that twenty-nine languages are considered minimum entry for a complete intelligence picture.[23]

Intelligence or knowledge, regardless of the origin of its precursor-information (open or clandestine), must be timely, accurate, relevant and verifiable.[24] It must answer a question and it must engender proactive actionable decision-making even if that decision is not to act. One of the criticisms of OSINT is that it is not easily verifiable or evaluated. This perception is particularly true of information derived freely via the Internet. It is a less expressed criticism of information derived from premium content sites, academic peer-reviewed grey-literature or ground truth experience. Like all sources of information, trust, the passage of time, and analyst expertise become the defining arbiters of value. Being in the public domain is not to be confused with being available to the public. There are barriers to entry, notably, money and effort. The exchange of information for money or endeavour, or both, still remains a potent validation of the worth of that information in a free market economy. The assertion that the value of intelligence represented by degree of classification is the defining mark is at best misguided and worst psychotic. Closed information displays a degree of sensitivity of the source, the method by which it was obtained or the intention for which it is being used not the value it affords the creation of knowledge, decision-making and action. The open source convention is to consider and review the following checklist for each and every open source:[25]

- *Authority* – does the source command respect from its peers or customers?
- *Accuracy* – is the source corroborated and benchmarked against other validated all-source material?
- *Objectivity* – does the source advocate or balance views? To whom does it link? Who or what does it represent?
- *Currency* – is it date/time/place/author-tagged for currency?

OSINT offers a lifeline to intelligence by allowing it the freedom to communicate and disseminate risk issues, thereby informing perception and creating trust. In its turn, intelligence, informing rather than formed, can offer a lifeline to the beleaguered – democracy, trust and freedom

- *Coverage* – is it relevant (i.e., adds to understanding) or is it just interesting or circular reporting?

OSINT is accepted practice in the private sector where it merges with knowledge management and competitive intelligence. It is becoming more sophisticated with specifically developed techniques, tools, evaluation procedures and expert training. It would seem sensible to conclude that if OSINT is such a significant and growing input to private sector decision-making then public sector defence and security (intelligence included) should sit up and take note. The issue for OSINT is no longer its validity or usefulness but rather how could it be developed, institutionalized and rolled out as a discipline common to government intelligence analysts and commercial knowledge workers alike.

OSINT's contribution

OSINT is both a product of and tool for dealing with all three forces driving contemporary change. Open source information is a front-end ingredient for the process of analysis by which intelligence or knowledge is created in support of decision and policy-making, whether it is in defence, security or any function of society. But in an age characterized by instantaneous, distributed, publicly available, open source information, uninformed decision-making arising from an inability to understand, harness and exploit the potential of this new breed of information becomes a significant security weakness. Information gaps create communication credibility challenges, which lead to mistrust and a destructive cycle of stigma, increased mistrust and further credibility challenges for all policy makers.[26]

Why is OSINT so good? This presupposes that it is good relative to something else and that 'something else' is traditionally held to be intelligence obtained through espionage. The more perceptive organizations that require knowledge to function are beginning to appreciate that the two are not in competition but mutually supportive. It has been estimated by many senior representatives of the intelligence community, that approximately 80 per cent of knowledge, upon which decisions are made and action is taken in the public sector, derives from OSINT.[27] The original source of this figure may very well have been Allen Dulles (former Director CIA), when in 1947 he made the following comment as part of his testimony to the Senate Committee on Armed Services, 25 April 1947:

> *A proper analysis of the intelligence obtainable by these overt, normal and aboveboard means would supply us with over 80 percent, I should estimate, of the information required for the guidance of our national policy.*[28]

His testimony was only nine pages long and hastily written; but in it, as Markowitz has noted, he began the process of the demystification of the art of intelligence.[29] Anecdotally, this figure may be nearer 90 per cent and, for some all-source intelligence agencies, is the preferred 'knowledge' of choice.[30] But 90 per cent of what? Is it 90 per cent of a final intelligence report or 90 per cent of action outcomes, i.e. an arrest or a threat interdiction? Whatever it is a percentage of, it remains a subjective judgment but its perceived efficacy by practitioners and more importantly satisfied customers is likely only to increase.[31]

At the level of intelligence *qua* process and product, and as an 'INT' in its own right alongside the clandestine 'INTs' (Humint, Sigint, Elint etc.), the main benefits of OSINT include the following:

- It is fast, flexible, dynamic and cheap;[32]
- It is communicable, sharable, trust creating and partner–forming, particularly for multi-national organizations such as NATO and the UN engaged in peacekeeping operations, where nationally-supplied intelligence has a restricted flow and therefore limited value;[33]
- It identifies and mitigates risk at strategic, operational, tactical and technical levels – 'horizon scanning' to sophisticated targeting;
- It spans 'quick and dirty' evaluation to in-depth analysis;[34]
- It contextualizes the intelligence requirement both historically and currently, providing the matrix in which the clandestine 'INTs' can set their nuggets of closed information, as well as the foundation upon which they can be more effectively and efficiently directed;
- It contributes to the all-source collection process of itself and by 'freeing-up' other 'INTs' for their own more concentrated espionage;

- It provides 'cover' and risk communication possibilities for the other 'INTs'; and

- It provides 'horizon-scanning' to focus the other 'INTs'. 'If it is 85 per cent accurate, on time and I can share it, this is a lot more useful to me than a compendium of TS [Top Secret] Codeword materials that are too late, too much and requires a safe and three security officers to escort it around the battlefield.'[35]

OSINT can usefully contribute to the wider management of risk by enhancing the informing of perception, where little or none exists, through utilizing risk communication theory and generating virtuous circles of trust and confidence rather than mistrust and stigma. Perception is moulded by a variety of factors including: how the information is framed for communication;[36] the bias or culture of the sender and receiver;[37] the amplification of the signal or groups of signals that form the message;[38] the 'availability heuristic' predisposing us to remember the most recent and/or most prominent signals;[39] and the theory of 'affect' which recognizes, amongst others, intuition, emotion and judgment in the formation of perception.[40] The more people know about the risks they face – provided that the informing has been balanced, honest, open and having preferably emanated from a trusted figure – the more likely they will be to cope, habituate and ultimately change behaviour.[41]

At the level of national and international policy and decision-making, OSINT will have its biggest role to play in generating resilience and competitive advantage. This would be achieved by habituating citizen-decision-makers to risks, reducing their fear and impotence and returning decision-making and its corollary, action, to those individual decision-makers. Where the management of complex, uncertain and ambiguous risk is concerned – from prions to 'dirty-bombs' – OSINT can be used to inform, educate and habituate the perceptions of those risks before, during and after they have occurred.[42] Equally, if and when these risks do occur, as we have been promised they will, then a concerted risk management continuity and recovery effort can be enhanced by the dissemination of useful information to the public through the media.[43] Before, during and after – the appropriate communication and dissemination of risk issues can in turn contribute to the preservation of democracy, trust and freedom or help reinstate it where it is lacking.

Conclusion

OSINT is not a new breed of intelligence per se. It is a common enough technique used by intelligence organizations in all sectors and by many generations of intelligence professionals. However, it is new to elements of the national intelligence and national security machineries in so much as it has been formally recognized and accorded its place by the relatively recent creation of open source intelligence cells and the appointment of open source intelligence specialists. Whether there is a strategy for its newly-elevated role in these machineries is of even greater interest. Is it worthy of single-source, collection agency status or should it be integral to all source analysis?

At a functional level, it is already setting the context in which the other clandestine 'INTs' can operate and be focused as well as contributing to strategic, operational, tactical and technical intelligence analysis in its own right. However, in a far deeper way, it is also responsive to the new forces shaping our contemporary society by virtue of being forged out of them and empathic with them. Where policy and decision-makers for resilience, security and defence must manage the complexity, uncertainty and ambiguity of the global, postmodern, risk society, OSINT offers a lifeline to intelligence by allowing it the freedom to communicate and disseminate risk issues, thereby informing perception and creating trust. In its turn, intelligence, informing rather than formed, can offer a lifeline to the beleaguered – democracy, trust and freedom. These should be the measures of the standing of intelligence, not Hutton. ■

NOTES

1. *This concern was expressed by speaker after This concern was expressed by speaker after speaker at the '2002/2003 Intelligence Seminar Series' at St Anthony's College Oxford.*

2. *Hutton Inquiry, http://www.the-hutton-inquiry.org.uk/ as at September 2003.*

3. *Tim Jackson and Laurie Michaelis, Policies for Sustainable Consumption: A Report to the Sustainable Development Commission (September 2003).*

4. *Andrew Rathmell, 'Towards postmodern intelligence', Intelligence and National Security, (Vol. 17, No. 3, 2002), pp. 87-104.*

5. *John Gray, Straw Dogs: Thoughts on Humans and Other Animals (London: Granta Books, 2002).*

6. *Samuel P. Huntington, The Clash of Civilizations and the Re-making of World Order (London: Simon & Schuster, 1996).*

7. John Adams, Risk (London: Routledge, 1995).

8. Unequivocally referred to by UN Secretary General Kofi Annan in his speech to the UN General Assembly, (23 September 2003). http://news.bbc.co.uk/1/hi/world/americas/3133364.stm

9. Robert Kagan, Paradise and Power: America and Europe in the New World Order (London: Atlantic Books, 2003).

10. Ulrich Beck, World Risk Society (Cambridge: Polity Press, 2001).

11. Paul Slovic, The Perception of Risk (London: Earthscan , 2000), and Francis Fukuyama, Our Posthuman Future: Consequences of the Biotechnology Revolution (London: Profile Books, 2002).

12. Benjamin Barber, Jihad vs. McWorld: Terrorism's Challenge to Democracy(London: Transworld, 1995).

13. Ibid.

14. Hence the setting up in 2003 of Project Unicorn, a joint public/private sector venture to explore better means of communication between the two sectors following the aviation industry's despair at hitherto lamentable levels of co'operation.

15. James Legge, Confucian Analects, The Great Learning, and The Doctrine of the Mean (Oxford: Clarendon Press, 1893).

16. Ronald Inglehart, 'Trust, well-being and democracy' in: Mark Warren (ed.), Democracy and Trust (Cambirdge: Cambridge University Press, 1999), pp. 88-120.

17. Ortwin Renn and Andeas Klinke, 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies', Risk Analysis (Vol. 22, No. 6, 2002), pp 1071-1094.

18. 'GM Nation? The Findings of the Public Debate', Agricultural and Environmental Biotechnology - Steering Committee Report (2003), (24 September 2003). http://www.gmpublicdebate.org/ut_09/ut_9_6.htm#download

19. Bill Durodie and Simon Wessely, 'Resilience or Panic? The public and terrorist attack', The Lancet, (Vol. 360, No.9349, 2002) pp. 1901-1902

20. Stevyn Gibson, 'OSINF: The Lifeblood of Decision-Making', RUSI/Jane's Homeland Security &Resilience Monitor (Vol. 2. No. 5, 2003), pages 6-8.

21. Yahya Dehqanzada and Ann Florini, 'Secrets for Sale: How Commercial Satellite Imagery will Change the World' in 'Open Source Intelligence Reader', NATO, (2002)

22. http://www.cartographic.com/xq/ASP/AreaID.33/RegionID.131/CategoryID.5/ProductID.2308/midd23e_east/iran/qx/topographic_maps.asp as at September 2003

23. Robert Steele, Peacekeeping Intelligence: Emerging Concepts for the Future, (2001).

24. This essay uses intelligence and knowledge interchangeably to mean the same thing. Intelligence professionals would not necessarily agree with the lack of distinction. Any differentiation requires much more space than this essay allows or its title suggests.

25. Open Source Intelligence Handbook, NATO (2001), and Intelligence Exploitation of the Internet, NATO (2002).

26. Vincent Covello, Peter Sandman and Paul Slovic, Effective Risk Communication: The Role and Responsibility of Government and Non-government Organizations (New York: Plenum Press, 1989).

27. There are numerous credible sources for this estimate; Lt Gen Sam Wilson (former Director DIA) Washington Times (17 November 1997), Ward Elcock (former Director of CSIS) cited in Government Information Quarterly, (Vol. 13, No. 2), pp 161, Professor Arthur S. Hulnick in International Journal of Intelligence and Counter-Intelligence (Vol. 15, No. 4), pp 565. Dr Paula Scalingi, Counter-proliferation organization, Los Alamos National Laboratory 1994.

28. Senate Committee on Armed Services, Hearings on the National Defense Establishment, 1st Session, 1947, pp 525-28, as recounted in Peter Grose, Gentleman Spy: The Life of Allen Dulles, (1994), pp 275.

29. Joseph Markowitz, Open Source Strategic Plan, US Community Open Source Programme, (1995).

30. Gibson, Op. cit., 2003.

31. NATO, EUROPOL, EU, UK MOD, Swedish MOD, Dutch MOD, US DIA, CIA, UK HM Customs & Excise to list a few in the public sector.

32. Robert Steele, On Intelligence: Spies and Secrecy in an Open World (OSS International Press, 2001).

33. Ben De Jong, Wies Platje and Robert Steele, (ed.) Peacekeeping Intelligence: Emerging Concepts for the Future (OSS International Press, 2003).

34. 'Open Source Intelligence Reader',2002.

35. US Navy Commander of the lead wing into Baghdad, 1991in Robert Steele, On Intelligence: Spies and Secrecy in an Open World (2001), p 105

36. Slovic, op cit., 2000.

37. Adams, Op cit., 1995.

38. Carlo Jaeger and Ortwin Renn, Eugene Rosa, Thomas Webler, Risk, Uncertainty and Rational Action, 2001.

39. Slovic, Op cit., 2000.

40. Ibid and C. Jaeger et al, op cit, 2001.

41. See T Brewin, 'Chernobyl and the Media', British Medical Journal (No. 309, 1994) pp.208–209; B. Modan, M. Tirosh, E. Weissenberg, C. Costin, T. A. Swartz, A. Donagi, C. Acker, M. Revach, and G. Vettorazzi, 'The Arjenyattah Epidemic—A Mass Phenomenon: Spread and Triggering Factors', Lancet (Vol. 2) pp. 1472–1475; E. Singer and P. Endreny, Reporting on Risk, Russell Sage Foundation, 1993; C. Jaeger and O. Renn, E Rosa, T. Webler, Op cit., 2001; and A. Mazur, 'Does Public Perception of Risk Explain the Social Responses to Potential Hazard?' Quarterly Journal of Ideology (Vol. 11, 1987), pp. 41-45.

42. Kenneth Hyams, Frances Murphy, Simon Wessely, 'Responding to Chemical, Biological or Nuclear Terrorism: The Indirect and Long-Term Health Effects May Present the Greatest Challenge', Journal of Health Politics, Policy and Law, (Vol. 27 No. 2, 2002), pp. 273-291.

43. Peter Bennett, David Coles and Anne McDonald, 'Risk Communication as a Decision Process', In Risk Communication and Public Health, P. Bennett and K. Calman, (Ed.), Oxford University Press, (1999).