CRANFIELD UNIVERSITY

STEVYN D GIBSON

OPEN SOURCE INTELLIGENCE: A CONTEMPORARY INTELLIGENCE LIFELINE

DEFENCE COLLEGE OF MANAGEMENT AND TECHNOLOGY

PhD THESIS

CRANFIELD UNIVERSITY

DEFENCE COLLEGE OF MANAGEMENT AND TECHNOLOGY

DEPARTMENT OF DEFENCE MANAGEMENT AND SECURITY ANALYSIS

PhD THESIS

Academic Year 2006-2007

Stevyn D Gibson

Open source intelligence (OSINT): A contemporary intelligence lifeline

Supervisor: Dr L Cleary

July 2007

ABSTRACT

Traditionally, intelligence has been distinguished from all other forms of information working by its secrecy. Secret intelligence is about the acquisition of information from entities that do not wish that information to be acquired and, ideally, never know that it has. However, the transformation in information and communication technology (ICT) over the last two decades challenges this conventionally held perception of intelligence in one critical aspect: that information can increasingly be acquired legally in the public domain - 'open source intelligence' (OSINT).

The intelligence community has recognised this phenomenon by formally creating discrete open source exploitation systems within extant intelligence institutions. Indeed, the exploitation of open source of information is reckoned by many intelligence practitioners to constitute 80 percent or more of final intelligence product. Yet, the resource committed to, and status of, open source exploitation belies that figure.

This research derives a model of the high order factors describing the operational contribution of open source exploitation to the broader intelligence function: context; utility; cross-check; communication; focus; surge; and analysis. Such a model is useful in three related ways: first, in determining appropriate tasking for the intelligence function as a whole; second, as a basis for optimum intelligence resource allocation; and third, as defining objectives for specifically open source policy and doctrine. Additionally, the research details core capabilities, resources, and political arguments necessary for successful open source exploitation.

Significant drivers shape the contemporary context in which nation-state intelligence functions operate: globalisation; risk society; and changing societal expectation. The contemporary transformation in ICT percolates each of them. Understanding this context is crucial to the intelligence community. Implicitly, these drivers shape intelligence, and the relationship intelligence manages between knowledge and power within politics, in order to optimise decision-making. Because open source exploitation obtains from this context, it is better placed than closed to understand it. Thus, at a contextual level, this thesis further argues that the potential knowledge derived from open source exploitation not only has a unique contribution by comparison to closed, but that it can also usefully direct power towards determination of the appropriate objectives upon which any decisions should be made at all.

ACKNOWLEDGEMENTS

I would particularly like to acknowledge the contribution of a now battered 1991 copy of T*he Concise Oxford Dictionary*, an even older and more battered 1968 copy of *The Nuttall Dictionary of English Synonyms & Antonyms*, together with their modern counterpart, but not replacement - the Internet.

I was fortunate to have two supervisors - Dr Laura Cleary and Dr John Robertson. I am most grateful to both of them. The former took over seamlessly from the latter for internal institutional reasons, although both were involved from start to finish. Their combined encouragement and support throughout was crucial. I am also grateful to Professors Chris Bellamy and Wyn Bowen who constituted my thesis committee. The former gave me fundamental inspiration to pursue the research, and the latter gave me invaluable additional subject matter expertise.

Finally, I would like to acknowledge the contribution of the various intelligence practitioners, who were prepared to engage in the research process with someone outside their natural community and thus outside their cultural comfort zone. Not only does this, of itself, reflect the sense of import attached to the formal exploitation of open sources of information, but it also reminds us that intelligence communities are formed from members of society not so wildly different from the rest of us. Yet, unlike the rest of us, they play an important part in the relationship between knowledge and power through their contribution to decision making on behalf of their respective societies. I hope that this thesis may be as useful to them in managing that sensitive relationship, as they have been instructive in forming it.

CONTENTS

LIST OF TABLES

LIST OF FIGURES

GLOSSARY

9/11	The popular shorthand for the four aeroplane-based attacks conducted against significant institutions in the continental United States on 11 September 2001
AD/DNI-OS	Assistant Deputy Director DNI - Open Source (US)
Agencies, the	SIS, GCHQ, and BSS – the three UK intelligence agencies that constitute the Single Intelligence Account
AKO	Army knowledge Online (US)
ASCC	Army Service Component Command (US)
ASD	Asian Studies Detachment, Camp Zama, Japan (US)
BBC (M)	BBC Monitoring (formerly BBC Monitoring Service)
BSS	British Security Service (formerly known as MI5
CDI	Chief of Defence Intelligence (UK)
CENTCOM	US Central Command, MacDill Air Force Base, Tampa (FL)
CESG	Communications Electronics Security Group (UK)
COCOM	Combatant Commands (US)
CONTEST	UK Counter-terrorism strategy
COSPO	Community Open Source Program Office; one of the first formally established OSINT organisations in an intelligence agency (US - CIA)
CSO	Civil society organisation
CSRC	Conflict Studies Research Centre (UK-based OSINT organisation, successor to Cold War SSRC)
DAC	Department of the Army Civilian (US)
DEJWG	Data Exploitation Joint Working Group (UK)
DIA	Defense Intelligence Agency (US)
DIS	Defence Intelligence Staff (UK)
DNI	Director of National Intelligence (US)
DOD	Department of Defense (US)

Dstl	Defence Science and Technology Laboratory (UK)
EA	Exclusive Analysis
EU	European Union
EUCOM	European Command (US)
EUROPOL	European Police Office
FBIS	Foreign Broadcast Information Service (US - forerunner to OSC)
FCO	UK Foreign and Commonwealth Office
FOIA	Freedom of Information Act
FMSO	Foreign Military Studies Office (US)
GCHQ	Government Communications Headquarters (UK)
HCR	Humint Collection Requirement (US)
HMRC - LE	Her Majesty's Revenue & Customs - Law Enforcement (UK), formerly Her Majesty's Customs & Excise (HMCE)
HMS	Hazard Management Solutions Ltd.
Humint	Human (sourced) intelligence
IA	Information assurance
IAEA	International Atomic Energy Agency
IC	Intelligence community
ICT	Information and communication technology
ICTY	International Criminal Tribunal for the Former Republic of Yugoslavia
IED	Improvised explosive device
IIR	Intelligence Information Requirement (US)
INGO	International government organisations
INSCOM	Intelligence & Security Command (US)
IOSWG	International Open Source Working Group: a 12-nation collaboration between national intelligence communities on open source exploitation
Intelink-U	Intelligence Link-Unclassified (US - replacement of Intelink-SBU)

Intelink-SBU	Intelligence Link-Sensitive but Unclassified (US - forerunner to Intelink-U)
ISC	Intelligence and Security Committee (UK oversight body for policy, administration and expenditure of UK IC, principally the SIA)
ISRC	Intelligence, Security and Resilience Co-ordinator (UK Permanent Secretary ranked civil servant - Chairman of the JIC as well as principle interface between JIC and government - successor to position of SIC)
JIC	Joint Intelligence Committee (final assessment body for UK intelligence analysis prior to submission to government and policy)
JTAC	Joint Terrorism Analysis Centre (UK)
JWICS	Joint World Intelligence Communication System (US - TS level)
Masint	Measures and signatures (sourced) intelligence
MI	Military Intelligence
MNC	Multi-national corporation
MOD	Ministry of Defence (UK)
MPS	Metropolitan Police Service (UK)
NASIC	National Air and Space Intelligence Center (US)
NATO	North Atlantic Treaty Organisation
NCW	Network-centric warfare
NEC	Network-enabled capability
NETCU	National Extremism Tactical Coordination Unit (UK)
NFP	Not for profit (organisation)
NGIC	National Ground Intelligence Center (US)
NIM	National intelligence machinery (more often a UK term)
NIPRNET	Non-secure Internet Protocol Router Network (US - unclassified level)
NGO	Non-governmental organisation
NHTCU	National High-Tech Crime Unit (UK - absorbed into SOCA 2004)
NPOIU	National Public Order Intelligence Unit (UK)

NSA	Non-state actor
OSC	Open Source Center (US national open source organisation)
OSCE	Organisation for Security and Cooperation in Europe
OSINF	Open source information
OSINT	Open source intelligence
OSIS	Open Source Information System (US)
OSJWG	Open Source Joint Working Group (UK) This body is the UK Intelligence Community's lead on all open source exploitation matters. Initially, it comprised just representatives of the three members of the Single Intelligence Account plus DIS. During 2005-7 membership extended to other public agencies; for example JTAC, SOCA and Cabinet Office. Additionally, other relevant attendees have been invited to attend; for example the author.
PACOM	US Pacific Command (US - based in Hawaii)
PHIA	Professional Head of Intelligence Analysis, who is also the 'Open Source Champion' (UK)
PIB	Private information brokerage
PICTU	Police Intelligence and Counter Terrorism Unit (UK)
PRA	Political Risk Associates
SASO	Soviet Army Studies Office run by the Foreign Military Studies Office at Fort Leavenworth for the US Army during the Cold War
Sigint	Signals (sourced) intelligence
SIA	Single Intelligence Account (UK grouping of SIS, BSS & GCHQ)
SIC	Security and Intelligence Co-ordinator (UK Permanent Secretary ranked civil servant principally interfacing between JIC and government - forerunner to ISRC)
SIP	Senior Intelligence Practitioner
SIPRNET	Secure Internet Protocol Router Network (US - Secret level)
SIS	Secret Intelligence Service (UK - formerly known as MI6)
SitCen	Joint EU Situation Centre

SOCOM	US Special Operations Command, MacDill Air Force Base, Tampa (FL)
SSRC	Soviet Studies Research Centre (UK-based Cold War OSINT organisation, predecessor to present day CSRC))
Techint	Technical (sourced) intelligence
TCSO	Trans-national civil society organisation
USARPAC	US Army Pacific (based in Hawaii)
UN	United Nations
VIC/APAN	Virtual Information Centre/Asia Pacific Network (US - based in Hawaii)
WBIL	World Basic Intelligence Library (WBIL)
WMD	Weapons of mass destruction
WWI	World War One
WWII	World War Two

CHAPTER ONE

INTRODUCTION

> "A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives."
>
> James Madison (1822)[1]

1.0 Introduction

The human being is an amazing phenomenon. To a very great degree it has mastered many of the limitations, euphemistically called nature, which once entirely constrained it. Occasionally, very recently, and albeit briefly, it has demonstrated through space flight that it can entirely escape those earthly limits. Similarly, as a species it has singularly transcended all others. A range of evolutionary circumstances contributed to this superiority: an opposed thumb; the neo-cortex or cognitive aspect of the brain; self-awareness; and a highly sophisticated social system for cooperating, amongst others. The resultant creation is an entity that can write its own history, deliberately plan for the future, and, for those few that have the luxury of doing both, generate and benefit from social, cultural, and technological progress in the present. This desire to plan for the future is a significant and determining characteristic of human development. Crucially, such decision-making and action is dependant upon the raw material of information to fuel it. This information is rarely perfect, either in the sense of being complete, or fathomable. Yet, this imperfect information, when collected and interpreted, forms a key resource in the process of decision-making and action that propels the species forward from the past into the future. That future is shaped, partly by those decisions and actions of the present, and partly by ambiguous, random and uncertain events that can prove serendipitous or misfortunate. Chance notwithstanding, and as Madison suggests above, this sophisticated species has the opportunity to broadly progress, rather than regress, on the back of the

knowledge it creates and utilises at that boundary between the known today and the uncertain tomorrow, if it so wills it politically.

Thus, it is the manipulation of this thing called information, in particular its sharing, that dispels ignorance in favour of knowledge and drives the engine of progress. However, it remains a manipulation rather than a rational processing, partly because another aspect of the brain, the limbic, governs emotion and endows the creation of knowledge with a social construct firmly directed by this notion of political will, and partly because life for this species remains engaged in confronting many unknowable chance outcomes. One version of this manipulation of information is intelligence, whose purpose for security ends, according to one of its most seasoned practitioners, is to organise information into knowledge that can be put to use.[2] Yet, even intelligence can be seen to comprise at least two important sub-species: one is the traditionally familiar closed or secret intelligence that aims to organise information from targets that do not care to reveal it; the other, and the principle subject of this thesis, is the product of the exploitation of open sources of information - open source intelligence.

Open source intelligence (OSINT) is the exploitation of information legally available in the public domain (see 1.7 below).[3] In 1947, Allen Dulles originated the proposal that open source exploitation constitutes 80 percent of final intelligence product.[4] His estimation is now widely accepted as fact by modern intelligence practitioners and commentators, with some even suggesting a higher percentage.[5] If correct, it suggests a significant contribution. Yet, how that figure is derived beyond an informed estimate, or what it means beyond an intuitive feeling, remains unclear. An expression of frequency absent of impact is to confuse efficiency with meaningfulness. Absent of connection with meaningful outcome makes it a somewhat meaningless figure. Whatever the true contribution of open source exploitation to final intelligence product, its proportion of resource, budget, manpower or recognition, by contrast, is widely held by the same practitioners to be significantly less than 80 percent.[6] Nevertheless, it might be reasonably suggested from the outset that, however intractable or meaningless such measurements may

be, open source exploitation, as part of a broader intelligence effort, punches above its weight. 'Why' and 'how' seem pertinent departure points for further investigation into the exploitation of open sources of information, its relationship with the broader intelligence function, and its connection with the contemporary context for intelligence itself.

Thus, this thesis explores the changing character of intelligence as a result of the formal incorporation of open source exploitation into the intelligence functions of security, defence and law enforcement organisations (often referred to as the 'intelligence community' for shorthand).[7] Specifically, it examines the contribution of the exploitation of open sources of information to final intelligence product and develops a model describing that contribution based upon a set of high order factors. The research is based upon case-studies of open source organisations that support national and international intelligence community organisations.[8]

The research is timely, given the increased interest in intelligence's relationship between knowledge and power following the attacks on the US mainland of September 2001 (9/11) catalysing the so-called 'global war on terror', the inquiries into intelligence surrounding the treatment of Iraqi weapons of mass destruction (WMD) prior to the invasion of Iraq in 2003, and the wider transformation in information and communication technology (ICT) over the past two decades. Perhaps, more importantly, it contributes scholarly research towards a theory of intelligence.

1.1 Research aim, question and objectives

The aim of this research is to explore how open source intelligence contributes to the conduct of intelligence.

As recently as 2007, Bean, summarised much of the contemporary 'angst' over where and how open sources of information should be exploited within the US intelligence community. He crystallised the gap that this research fills:

> "Yet, the fact is that where the demarcation line between "information" and "intelligence" is drawn has much to do with stakeholders persuasive appeals, and less to do with any intrinsic quality of the information itself."[9]

The 'intrinsic quality' of open source exploitation is at the heart of this research effort, and a working hypothesis was assumed from the outset that this quality might be discovered and described.

1.1.1 Research question

What are the key high order factors that describe the contribution of open source exploitation to intelligence?

1.1.2 Research objectives

- A comprehensive review and analysis of the relevant literature in order to establish the historical, political and contextual sensitivities of the research problem, as well as demonstrate the demand for such a project.[10]
- A critical study of research methodology in order to apply the most appropriate research design.
- The development of a model describing the specific contribution of OSINT based upon data collected against a selection of OSINT cells and OSINT practitioner case-studies.
- Examination of a refined model against a case-study preparation in order to develop theoretical generalisation.
- To make conclusions about the model's theoretical generalisation and make recommendations for policy.

1.2 Scope of the research

The scope of the research is not so critically determined by geography, sector or culture but more self-selecting by its own richness of experience and quality of data sources. These are more likely to generate insight and understanding of the treatment of OSINT and its consequences for intelligence than restriction to a homogenous sample. Indeed, neither the practice nor the practitioners of OSINT are uniform - geographically, longitudinally, or within communities. For example, at the outset of this research, in the UK, Her Majesty's Customs and Excise OSINT organisation was approximately 80 strong, while the UK Metropolitan Police Service (MPS) dedicated only two people to OSINT.[11] In the US, the only clear example of a formally constructed OSINT cell within the closed intelligence effort of the US Armed Forces was the United States Special Operations Command (SOCOM) at ten strong.[12] By the end of the research, each of the nine US military Combatant Commands (COCOM) had instigated open source efforts to some degree. Yet, one case-study - the European Police Office (EUROPOL) - had effectively 'wound-up' its OSINT effort by the end of the research. The common phenomenon is open source exploitation itself.

OSINT exploitation within the national intelligence machinery is by no means confined to the US and UK. The Scandinavian countries, together with Holland, South Africa, Japan, Italy and Australia have all embarked upon OSINT exploitation to some degree.[13] However, like intelligence itself, there has been no research to explore any international comparison.[14] Furthermore, OSINT is also exploited by commercial, academic, intergovernmental and civil society organisations as well as public sector. Some of these would not recognise the term OSINT but effectively it is what they do to support their decision-taking and policy-making. While they do not necessarily have access to clandestine collection resources and may not subscribe to an intelligence secrecy ethos, but a commercially confidential one, the ICT transformation has nevertheless empowered them to exploit open sources of information. Deibert describes such non-state actor intelligence as 'network intelligence'; simply predicated on evolving computer network capabilities.[15]

The research study is aimed at the relationship between OSINT and the broader conduct of intelligence. Generally, the exploitation of OSINT by national intelligence machineries has the following common characteristics:

- It is security, law enforcement, or defence related; or a combination of all three
- It is formally established as a discrete cell and then 'spread' wider
- It is predominantly a 'developed' nation rather than universal phenomenon[16]
- It is 'connected' in some way to closed source intelligence

This latter point is most important in terms of the scope of this study. Odom alludes to the fact that US intelligence has never truly been evaluated in a way that other public sector organisations are.[17] Treverton argues that the only true value of closed intelligence is the comparison against what is openly available.[18] In this regard, members of the UK's Open Source Joint Working Group strongly reflect the use of OSINT as a check and balance upon their closed output. As will be shown in the model development chapter (Chapter Four) the efficacy of OSINT and closed source intelligence are increasingly being seen as mutually dependent. Therefore, the first key cut-off for this study is the combination and interaction of closed and open sources working together. Thus, it is critical that OSINT is examined within the context of an entire intelligence collection spectrum. This essentially limits the research to the US, UK, France, Russia, China, and international bodies that have access to these countries all-source intelligence assets.

It must also be stated that gaining access to these organisations was not easy, nor was the uniformity of access constant. Indeed, the practical access challenges, which reflect the very nature of secret and compartmentalised intelligence, had to be considered in case-study selection. Given the access difficulties to France, Russia and China, it seemed sensible to concentrate on the US, UK, and international bodies. Furthermore, the research was not intended to be experimental and hypothesis testing in any positivist sense, with precisely similar 'experiments' spread across the laboratory bench; their individual

variables regulated by minute fractions. Rather it was inductive and theory generating to derive rich understanding. Table 1.1 depicts what is in and what is out.

Table 1.1: Scoping table - in/out

OUT		
	NON - OPEN/CLOSED SOURCE COMBINED AGENCIES	
NON - DEFENCE NON - SECURITY NON - LAW-ENFORCEMENT NON - INTELLIGENCE RELATED ORGANISATIONS	**IN** **UK/US/International/private organisations producing or consuming open source intelligence**	INACCESSIBLE AGENCIES
	NON-DISCRETE OSINT CELLS	

Source: Author

The scope of this research will reflect these core characteristics by selecting qualifying examples for case-study preparation. However, the selection of national intelligence and law enforcement open source exploitation efforts does not preclude supplementing these case-studies, where appropriate, with leading contributors to the exploitation of OSINT such as private information brokers,[19] multi-national security organisations,[20] and leading individual intelligence community representatives and practitioners[21]. These organisations and individuals are often closely linked to, if not directly in support of, national security secret intelligence efforts anyway.[22] The final model, discussion, and conclusions are undoubtedly oriented towards the UK and US intelligence community, although they find resonance with other intelligence communities, where open source exploitation is concerned.[23] Finally, it is worth stating that the research is not aimed at the sources of information themselves. By definition, these sources are theoretically common to all, not just OSINT practitioners. It is what these practitioners do with them that is of interest here.

1.3 Research methodology

After the literature review, which precisely establishes the gap in our knowledge of exactly how open source exploitation contributes to the intelligence function, detailed in Chapter Two, the second critical objective is to ensure that an appropriate research methodology is adopted to fit both the philosophical position of the researcher and the needs of the research topic.[24] The guiding methodology adopted, based upon Straussian grounded theory[25], is summarised by Silverman's designation - analytic induction.[26] It is an iterative generation of theory aimed at reformulating and refining an initial hypothesis or model.[27]

The research problem is centred on the intelligence community's treatment of OSINT and uses case-studies within and in support of that community from which to extract relevant data. It is aimed at the changing conduct of intelligence as a consequence of the OSINT phenomenon. The research question specifically addresses the creation of a model that describes open source exploitation's contribution to intelligence. The nature and context of the research topic is more disposed to a phenomenological approach than a positivist one. There has been little research conducted in the field, thus, the research is exploratory and descriptive rather than explanatory or predictive. The aim is to generate theory rather than test hypothesis.[28] Therefore, meaning, insight and understanding are more pertinent at this stage in the subject's own development than frequency, measurement or causality.[29] By implication the logic or direction of the research methodology is inductive: development of theory from observation, rather than deductive: the testing of theory by measurement. Similarly, the research is qualitative rather than quantitative in order to avoid reductionism and enhance interpretation. The outcome of the research is designed to improve understanding as the contribution to knowledge rather than the solution of a problem. It is thus also pure or basic research rather than applied.[30]

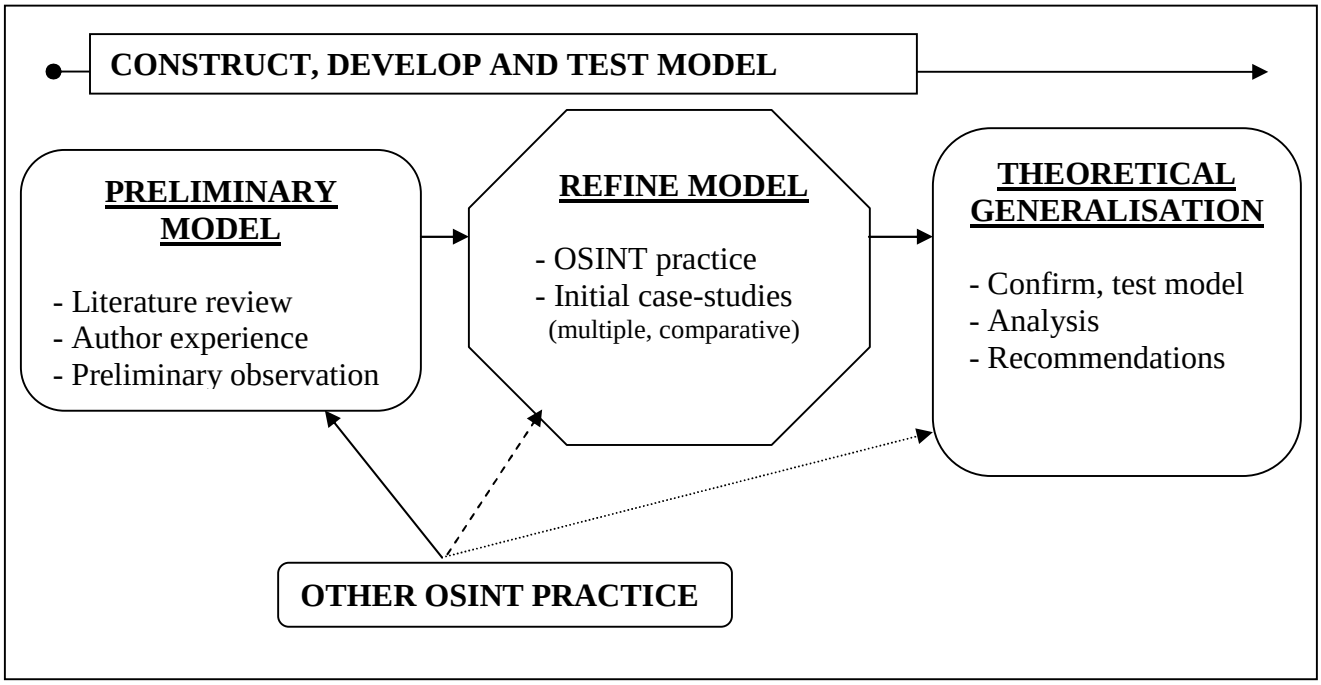
The researcher's philosophical position is firmly anchored towards the phenomenological end of the research paradigm continuum.[31] Specifically, it equates with a social-constructionist view of reality.[32] That is to say a belief in a world constructed by social

interaction as much as objective reality; subjective perceptions of reality are as valid as the 'truth' of that reality. Interestingly, this marries up well with one of the driving paradigms of contemporary society - risk - which demands as a central theoretical precept, that it has both an objective reality and a subjectively assessed construct.[33] These concepts are expanded in the literature review (Chapter Two) and methodology chapters (Chapter Three).

1.4 Research design

The question at the centre of the research study is to define a model of the high order factors, which describe the contribution of open source exploitation to the broader intelligence function. This is achieved by examining the literature, exploring a variety of OSINT practitioners, and conducting comparative case-study research across OSINT cells within and in support of intelligence organisations and the wider intelligence function. There are essentially three overlapping parts to the study. First, the development of a preliminary model based upon a review of the literature, preliminary observation, and enquiries of the intelligence community. Second, refinement of that model against a wider sample of OSINT practices. Third, the preparation of a final case-study to test the model and allow theoretical generalisation. An overview of the research design is at Figure 1.1.

Figure 1.1: An overview of the research project



Source: Author

1.5 Contribution to knowledge: Study value

There is little or no substantive body of academic research work on the exploitation of open source for intelligence purposes beyond the odd peer-reviewed paper or book chapter.[34] There is a vast practitioner literature, although it has largely been dominated by the tireless but somewhat evangelical work of Steele. This situation largely remained the case until 2005, when other work became increasingly available, pursuant to an increased attention, practical and theoretical, to open source exploitation by US and UK nation-state intelligence communities (see Chapter Four, in particular 4.2.6). By contrast, there is considerable and varied academic work on the broader subject of intelligence, as understood in terms of government purposes. This has been conducted principally from the purviews of political science and historical analysis, and all such enquiry has been invigorated by 9/11 and the Iraqi WMD question in order to re-analyse the purpose of

intelligence in the contemporary world. This thesis contributes to both academic and practitioner camps.

There are five ways in which this research represents a contribution to knowledge:

- It is the first time that any academic research has been conducted into the deliberate and formal exploitation of open sources for intelligence purposes within and across contemporary public intelligence and security agencies.
- It establishes a model describing the high order contributing factors of this exploitation to the broader intelligence function.
- It shows that open source exploitation has developed in the absence of any formal national policy and doctrine and makes some recommendations accordingly.
- It posits that open source exploitation - itself a reflection of the changing contemporary environment - might usefully form the lens through which the intelligence community can understand a changing world, if not itself.
- It makes some contribution to a theory of intelligence by drawing distinction between the nature and character of intelligence, and then further contends that notions of secrecy and the cultural obsession with classification should no longer dominate the classic definition of intelligence in contemporary times.

When this work was started the author was partially seduced by the notion that the exploitation of open source intelligence would change intelligence. That now seems a rather arrogant thought. The nature of intelligence has not changed. It remains to support decision makers. However, its character is always changing, and the exploitation of open source is certainly at the heart of that evolution. Indeed, it is evolution and change that should more realistically reflect and direct the conduct and character of intelligence. The terms reform and revolution are unhelpful, distracting, 'waspish', and easy. They are by no means the be all and end all of intelligence debate. Thus, what is not demonstrated in this thesis is any new understanding of the nature or purpose of intelligence. Rather, it is an understanding of its changing conduct or character. In short the background theory of

open source exploitation is now placed upon a firmer footing through the focal theory of this research - how it contributes - than it was before.

1.6 Background to the research subject

The timing of this research contributes to its relevance. 9/11 has delivered western polities, and by implication their intelligence communities, a new focal purpose for the age - terrorism. Additionally, 9/11 and the rationale for the 2003 Iraq War have catalysed extensive examination of the intelligence function. History, and a longer view than can be offered in this thesis, will be the judge; yet, it already seems possible to view the very short period of time between the early 1990s and 2001 as a period of significant change for humanity in which 9/11 might come to be seen as a culminating reference point rather than any new departure.

Perhaps, more importantly, this was a period in which some significant geo-political and socio-cultural drivers consolidated their influence upon contemporary society. This thesis argues that globalisation, 'risk society', and changing societal expectations were three that became influential. Rooted in each of these influences is the transformation in ICT. It is these deeper influences, notably globalisation - as Aldrich with specific regard to intelligence has argued[35] - that are genuinely shaping our context; not 9/11, not Iraqi WMD, and not terrorism. As will be articulated throughout this thesis, globalisation, risk society, and changing societal expectation are pertinent to intelligence because they contribute to its context. And, as has been argued elsewhere, OSINT might well represent a 'lifeline', if not a unifying thread, for the understanding and management of these contextual influences, broadly because it is a product of them.[36]

Similarly, intelligence does not operate in a vacuum. Scholars in the field of intelligence studies note the transformation of Cold War intelligence from a secrecy-dominated puzzle-solving ethos into a more nuanced but uncertain understanding of adversarial mysteries and

intentions in a contemporary world characterised by 'transnationalism'.[37] Some commentators argue that mysteries and secrets have swapped over, in that, where once we knew capabilities but were unclear of intentions, we now know intentions but are unclear of capabilities.[38] Others suggest that it is even less clear; the advocates of the contentiously labelled 'Islamic-inspired' terrorism do not themselves fully understand, control or articulate what they do in its name.[39] Simultaneously, the sphere of interest of intelligence and security communities has expanded into broader risk categories that range from climate change to pandemics. They all broadly assert that we live in a time of profound change variously described as revolution, postmodernity, pre-politics, post-politics, and risk society to mention a few.[40] This change, if not carrying all in its path, certainly 'touches' all.

Yet, regardless of change, the function of intelligence because of its relationship with government, as Gill and Phythian have noted, confers upon it the status of 'mediator' through which power and knowledge is coordinated for political purpose.[41] Yet, these deeper drivers of contemporary society are also transforming the traditional notions of political purpose. Some argue that this transformation is resulting in a vacuum at the heart of politics; politics as originally conceived during the Enlightenment to be founded on the rejection of fate, a belief in human self-determination, and the pursuit of notions of reason, progress, and universal ideals, through argument and debate.[42] This thesis tackles OSINT's contribution to understanding the wider societal context, by which intelligence organisations might meaningfully and genuinely fulfil its side of the relationship with power and purposeful politics.

1.7 Open source intelligence (OSINT): the changing character of intelligence

Lowenthal describes open source intelligence as all information that can be derived from overt collection that entirely meets copyright and commercial requirements.[43] This might usefully be interpreted by way of definition from the outset as: the product of the

exploitation of information legally available within the public domain. It does not mean that it is free, easily available, in English, on the Internet, or indeed any of those things.

Within many national intelligence machineries, OSINT is increasingly recognised as a distinct and separate source similar to the more traditional clandestine sources such as human intelligence (Humint) and technical intelligence (Techint), although, it has not warranted a separate agency or discrete discipline, in the way that these other sources have been broadly designated.

OSINT has always been exploited; but it is a relatively new discipline in so far as formally incorporating and organising it within the intelligence function is concerned.[44] The first literature recognising this formal incorporation and organising of cells to exploit open sources began to appear in the mid-1990s commensurate with the establishment of discrete OSINT cells in national intelligence agencies such as the Community Open Source Program Office (COSPO) established in 1994 in the CIA run by Dr Jo Markowitz, as well as international collaboration between them such as the International Open Source Working Group (IOSWG) from 1995 onwards.[45] The extraordinary evolution of information and communications technology (ICT) in the last decade of the 20th century has forced its formal exploitation onto the traditional intelligence community.[46] Yet, its value has been intuitively perceived rather than expressly articulated. Because it was there, because we could, and because it supplemented and counterbalanced closed or secretly acquired information, were considered sufficient warranty for its exploitation.

Thus, while open source exploitation is clearly undertaken, it is not clearly understood why. In the 'balkanised' structure and secrecy-dominated culture of the intelligence community it has not easily demonstrated its efficacy as an intelligence source, either absolutely in its own right or relatively to other sources, in any uniform way. Until very recently, with the arrival of open source champions in the UK and US in 2005, OSINT has been pursued piecemeal within organisations across the intelligence community, rather than collectively as a source or independently as an agency in its own right.

Indeed, it is difficult to precisely categorise open source exploitation. It underpins all the individual secret disciplines, and is often uncharitably regarded as a 'poor-man's' all-source capability. It can be viewed as a technological platform aimed at the all-source product in much the same way that the exploitation of satellites by the early 1960s gave rise to the undisputed Cold War heavyweight champion of technical-intelligence collection - satellite imagery. In this regard, it might be foolish to confer 'agency' status upon OSINT, when it is clearly ubiquitous in application and outcome. Yet, it is a more abstract, holistic, and capable intelligence platform than the satellite. OSINT can direct its own collection product, which in turn can be analysed to produce intelligence independent of any other collection format, and is theoretically available to anyone who wants it. Thus, an appropriate treatment of open source exploitation remains unclear.

This study confirms that the treatment of OSINT in the intelligence community remains irregular both within and across its intelligence organisations. Structurally and procedurally, it is varyingly resourced, supported, understood, trusted, positioned, and utilised. Culturally, several contributory factors militate stubbornly against a comprehensive approach and are reflected extensively in the literature:

- The prevailing culture of secrecy that dominates its intelligence setting inevitably clashes with openness.[47]
- An unwillingness to completely engage with the total information business militates against exploiting anything other than 'closed' information.[48]
- A belief that the 'intelligence community' alone has the preserve on knowledge creation obstructs its exploitation of open sources of analysis.[49]
- An apparent inability to reflect contemporary society's critical paradigms - globalisation, risk and changing societal expectation.[50]

But, this study also recognises that intelligence communities know this too, and have most recently, post the contemporary inquiry season, taken steps to adjust.

1.8 The changing context for intelligence: Nature versus character

The transformation in ICT and the deeper geo-political and socio-cultural shifts that ICT abets are changing the context, which define our security threats, as well as our response to them. Ideological, nation-state, fixed, belligerent, human-originated threats have been replaced, temporarily perhaps and in the main at least, by politically ill-defined, asymmetric, global risks of human and non-human origin. For intelligence communities this has meant a realisation that they are engaged with a complex rather than merely complicated world; that they are engaged in mystery understanding rather than puzzle solving. Whether this new context is more perceived than real is an important distinction and discussed further in Chapters Two (2.2.2) and Five (5.2.2).

Attempts to define intelligence have proved notoriously difficult endeavours. This thesis applies a useful argument to intelligence, articulated by Gray with regard to war, which distinguishes the character or conduct of a phenomenon from its nature or purpose; its grammar from its logic respectively.[51] With regard to intelligence, the purpose - why - of intelligence is to support decision-making. The conduct of intelligence - how - is the combination of inputs, outputs, process and environment required to achieve that purpose. Thus, it is the character of intelligence that should reflect this changing context not the nature.

The 'dissatisfaction' with the capability of national intelligence machineries to effectively support their policy masters was the received wisdom concluded by the spate of western intelligence inquiries following 9/11 and, particularly, the 2003 Iraq War. Such ineffectiveness has been variously debated and attributed to part intelligence failure, part politicisation, or some combination thereof. Whichever part of that spectrum one occupies, it reinvigorated the periodic debate on intelligence reform. By 2004, not only was the intelligence function perceived broken, certainly the 'western' version, but it was also perceived discredited.[52] The manifestation of the 2000's version of intelligence crisis came to be represented by:

- The notion of 'scandal' including: the incorporation and plagiarising of parts of a PhD thesis into UK national intelligence assessment - the so-called 'dodgy-document';[53] the death of Dr David Kelly; and the inconsistency of assessment of the Niger uranium source.[54]
- The notion of 'group-think', whereby intelligence agencies and their policy masters collectively developed, reinforced and set in stone an assessment of Iraq's engagement with Al Qaida and WMD capability that has proved difficult to sustain as yet.[55]
- The notion of 'politicisation', whereby, 'western' intelligence, like its non-western cousins, mal-appropriated intelligence in order to enforce policy rather than inform it.[56]

However, these and other conclusions refer to the conduct of intelligence and why it 'fails' rather than its nature. Suffice to say that as part of the 'correction' process, the significance of open source exploitation was once again recognised.[57] In the US, the 9/11 Commission Report recommended the formation of an open source capability within the intelligence community.[58] The US House/Senate Report went further, albeit confirming the dilemma of where to place OSINT, when it recommended that: "Each element of the intelligence community uses open source intelligence consistent with the mission of such elements."[59] These recommendations were reflected in legislation in the US Intelligence Reform Act of December 2004:

> "It is the sense of Congress that the Director of National Intelligence (DNI)[60] should establish an intelligence center for the purpose of coordinating the collection, analysis, production, and dissemination of open source intelligence…"[61]

In November 2005, this commitment was most clearly demonstrated by the creation of the Open Source Center (OSC) under the auspices of Assistant Deputy Director National Intelligence Open Source (AD/DNI-OS) Eliot Jardines, with direction going to the Head of the Foreign Broadcast Information Service (FBIS) Douglas Naquin, effectively the base for the new OSC. Similar 'recognition' of open source exploitation in the UK was less public with the creation of an Open Source Champion in 2005, moreover, as is noted in

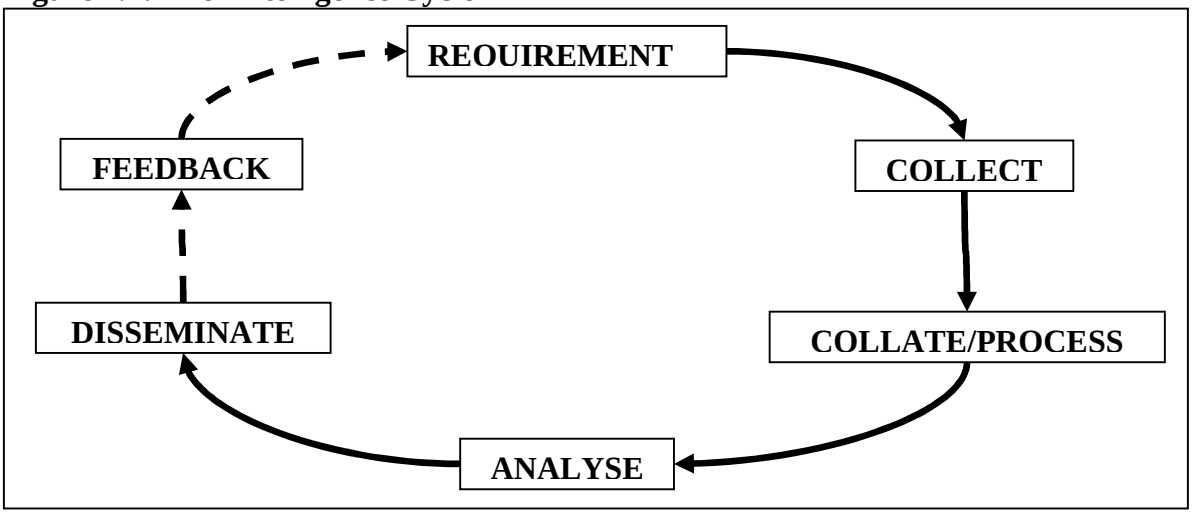
Chapter Four (4.2.6), already in place in the form of the Open Source Joint Working Group (OSJWG) since 2000.

1.9 Intelligence process: Old models and new models

> "A nation's best defense is an educated citizenry."
>
> Thomas Jefferson, 1801

The intelligence process is steadfastly based upon the model of the 'Intelligence Cycle'.[62] It is a highly generalisable model, which continues to underpin all teaching on intelligence. However, its circular processional nature disguises its sequential linearity. It is effectively a straight-line process, which Treverton argues has become inappropriate for the speed of the networked world as, in practice, the strain of conforming to the order of things leads to it being 'short-circuited'.[63] Furthermore, it was conceived, and is geared, towards the process being carried out in an hermetically sealed box or 'closed' environment framework. Nevertheless, as a guide to the general idea behind the process of intelligence, it remains a valid and useful start-point. See Figure 1.2.

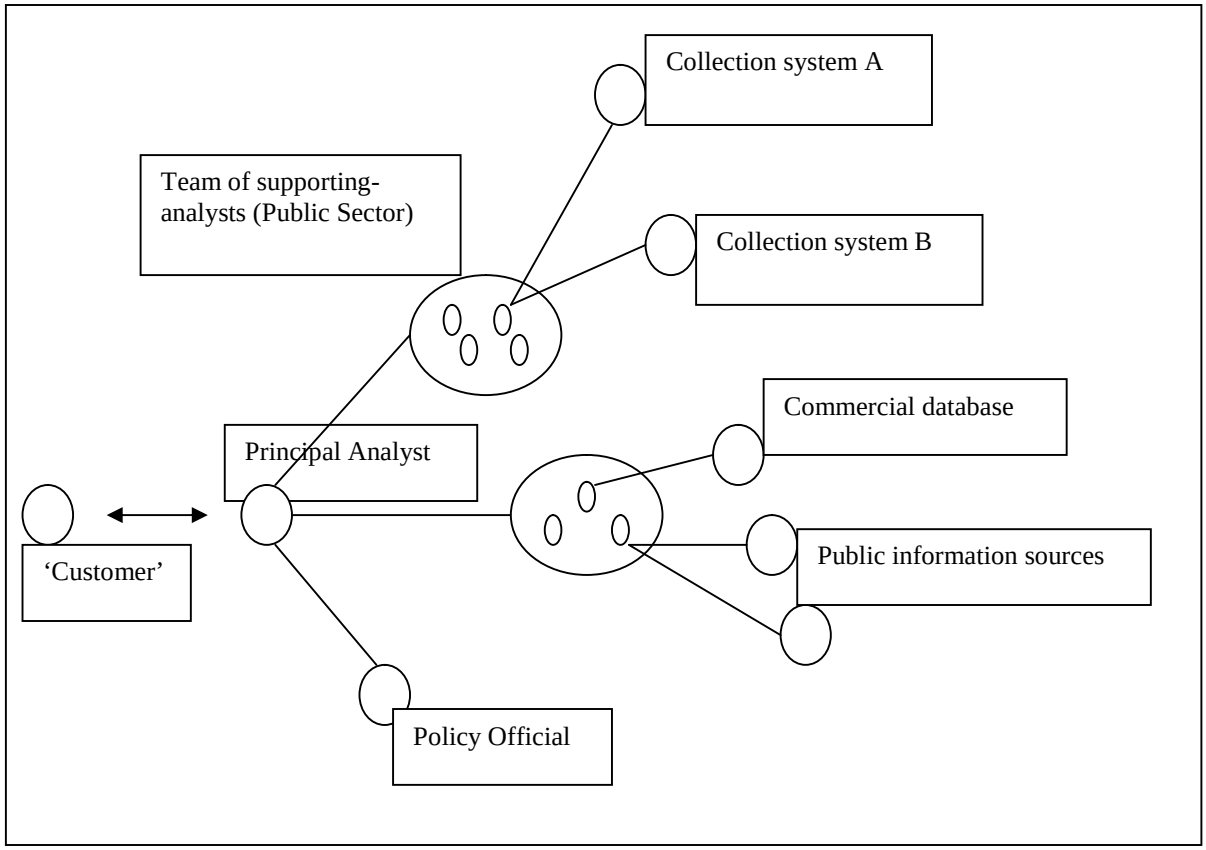
Figure 1.2: The 'Intelligence Cycle'



Source: Adapted from Krizan, 1999.[64]

Berkowitz and Goodman advocate that the closed environment in which intelligence is conducted is being superseded by a more 'network-centric' approach, which reflects both the strain on the intelligence process as cycle and the contemporary opportunity to exploit sources outside the closed environment.[65] As such it reflects the influence of the ICT transformation and the pertinence of open source exploitation. One might more usefully picture a model of the intelligence process as one of nodes inside each of which the intelligence cycle is discretely conducted. See Figure 1.3.

Figure 1.3: An alternative 'Network-Centric' model for the intelligence process

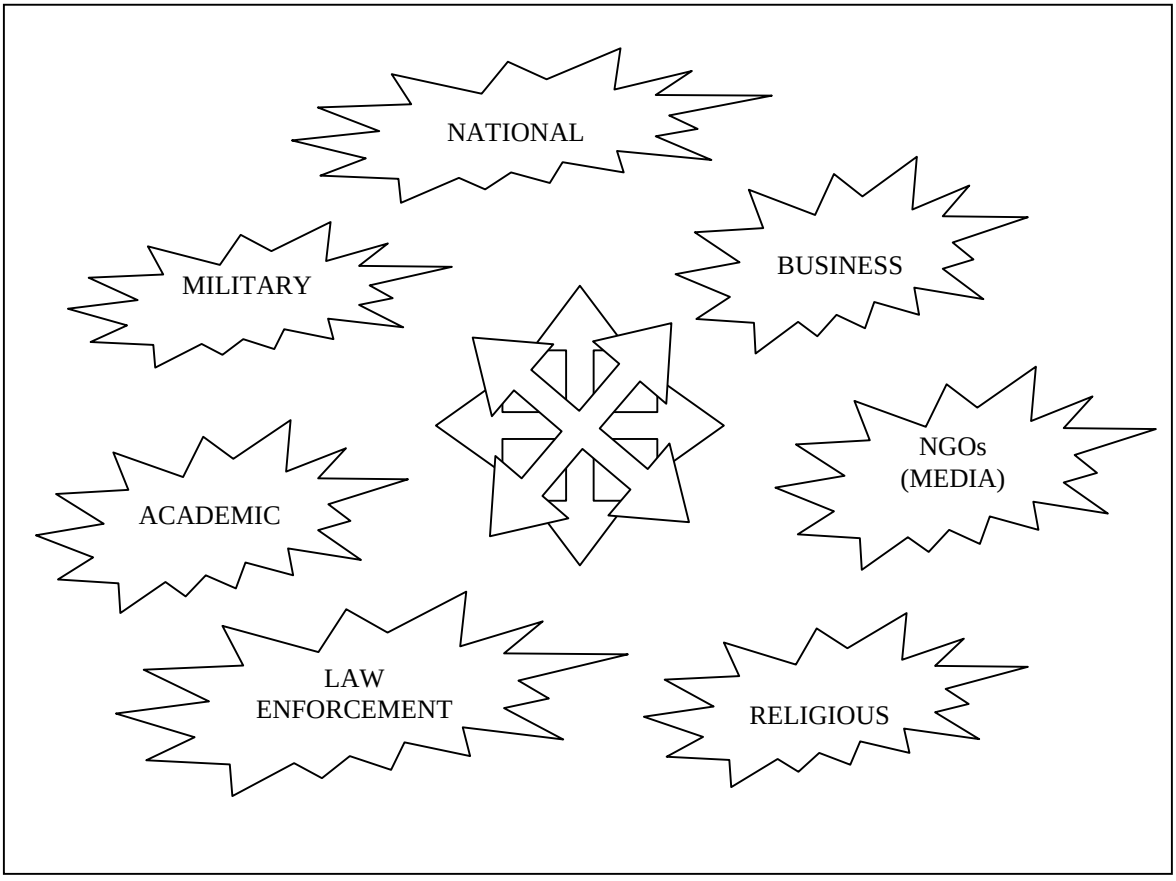


Source: Adapted from Berkowitz and Goodman, 2000.[66]

The only model for intelligence predicated specifically upon OSINT is Steele's 'intelligence commons' model. His approach, if not ethos, might best be characterised by Thomas Jefferson's laudable quote above. Steele's model describes how the exploitation

of the ICT transformation through OSINT might usefully unify all sections of society into an educated citizenry.[67] Again, within each of the sectors, it is argued that the intelligence cycle is the guiding model for how to 'do' intelligence.[68] Arguably it is simply the network-centric model writ large, but the sentiment - outside a closed environment - remains the same. It rather relies upon OSINT as 'heavy-lift' for much of the common networking effort. See Figure 1.4. The significant contribution of Steele to open source exploitation is discussed further in the literature review.

Figure 1.4: The 'Intelligence Commons'



Source: Adapted from Steele, 2001.[69]

1.10 Wanted: An understanding of OSINT's contribution

> "In the end, the US Intelligence Community will reach consensus about the who, what, where, when, why, and how of OSINT operations."
>
> US Army Field Manual Interim, 2006[70]

The prevailing environment of the intelligence community is predicated on the culture of secrecy. Secrecy is traditionally connoted with the security requirements of the techniques, sources, and intentions of the intelligence function. Yet, more often than not, secrecy belies a political culture and structure across the intelligence community that seems, at least, more concerned with internal competition than achieving ends. Whether security or secrecy is responsible, secret intelligence product is often rendered unusable because of its ultimately 'closed' nature. In an age when communication is immediate and vital for the political classes, at whatever level, a closed culture and structure delivers impotence and vulnerability as much as security. Open source exploitation, by definition, has an implied chance to circumvent if not puncture the secrecy culture.

Thus, the intelligence community, partial converts to the efficacy of OSINT, may fail to reap its maximum benefit as it is currently constructed and treated within the intelligence function. The traditional and extant intelligence function has absorbed OSINT as just another source. In order to determine a more optimal configuration it is necessary to explore how it is treated now, and theorise as to how it might be developed. One vision of a future for intelligence might centre on OSINT as the parent matrix in which traditional, closed, clandestine intelligence sources are set and focused.[71] Another might see it as entirely separate and distinct.[72] But first it would be useful to understand exactly how it contributes. Thus, OSINT's exploitation both of itself and for its significance in a wider intelligence context deserves examination.

The one true and final role of intelligence is to tell truth to power.[73] In the contemporary security context it is Johnson's description of truth as being honest with policy-makers that compliments Lowenthal's description of truth as an absolute and therefore unobtainable

commodity.[74] If intelligence cannot tell truth to power as best possible at least, if not absolutely, because its systems will not let it or its collective cultural mindset does not 'get' the way the world is, then it will move from being merely discredited and difficult to actually irrelevant and dead. OSINT addresses two fundamental drivers of the near intractable nature of contemporary intelligence practice. First, it can relieve the strains of the culture of secrecy. It is this institutional culture, the balance between security and sharing, which serves as nothing more than a stranglehold on the truth that intelligence is set to find. Second, it reflects the context of contemporary global risk society transformed by advances in ICT and science and technology. Because OSINT is 'of' that world and 'understands' it, it is perhaps best placed to contribute towards managing it. Acceptance of these two premises might only be a change in mindset away.

1.11 Thesis structure

The remainder of the thesis is structured to follow the iterative nature of the research methodology:

- **Chapter Two - 'minding the gap'**

  In surveying the landscape of intelligence, a review of the relevant literature establishes the context for the research problem.[75] It indicates that the exploitation of OSINT has hardly been explored beyond the practitioner literature. Thus, the first objective of establishing a need for this research is achieved. It identifies existing intelligence models and frameworks from the literature that can be brought to bear upon OSINT. However, these models are not specifically related to OSINT and do not develop an understanding of its place within the intelligence function. Thus it exposes a gap in how intelligence should treat OSINT and how intelligence is changing as a result of OSINT. It further demonstrates how OSINT is related to the wider debate on intelligence reform as well as contemporary societal issues.

- **Chapter Three - ‘an appropriate methodology’**

  This chapter discusses research methodology as philosophy and practice. It compares the author’s worldview - phenomenological - with the nature of the research subject in order to derive an optimum strategy - case-study - for the design of the research project. It describes how data are collected, triangulated and analysed.

- **Chapter Four - ‘data capture’**

  The literature review presents an initial set of descriptors representing the contribution of open source exploitation. It is the departure point for the data capture phase of the study. First, these descriptors are taken forward to contrast and compare with data captured from a set of preliminary enquiries into organisations that use both closed and open sources for intelligence purposes. This allows the author to set up a preliminary model of the contribution of open source exploitation. Second, this model is then refined against a selection of case-studies, where open source exploitation is the principle activity. Finally, the model is tested against a single in-depth case-study of a dedicated ‘stand-alone’ open source organisation feeding into a predominantly closed intelligence community. In all cases data are captured by indirect participant observation within organisations and semi-structured interviews with informants.

- **Chapter Five - ‘which truth, to which power, about what, from whom’**

  This chapter analyses the implications for policy of open source exploitation and the high order contributing factors that it lends to the broader intelligence function. It further discusses the relationship between open source exploitation and the context that shapes it. It raises wider implications for politics let alone intelligence.

- **Chapter Six - ‘conclusion’**

  The final chapter summarises the research as a whole. It notes the key findings, the contribution to knowledge, unresolved issues, and makes recommendations for open source policy and further research.

1.12 Summary

This thesis will argue that the exploitation of open source information contributes support to decision and policy-making on two levels. First, at an operational level, it is an increasingly specialised discipline that contributes in a discrete way to the intelligence function. The purpose of this research is to describe why and how that contribution is effective. Second, and perhaps more significantly at a contextual level, it can usefully inform a moribund polity of the deeper paradigms that are influencing all of society, which it perfectly reflects and encapsulates itself.

The exploitation of open source information may prove to be a most useful phenomenon upon which the conduct of intelligence might evolve. If not helping us to survive in our contemporary environment, it may be instrumental in questioning how new this environment really is. However, before open source exploitation can be granted such exalted status, it seems pertinent to understand exactly why and how it is effective.

References and Notes:

[1] Madison, J., 1822, in a letter to W.T. Barry dated 4 August 1822, as cited in Kurland, P.B., Lerner, R., (Eds), *The Founders' Constitution*, University of Chicago Press, Chapter 18, Document 35, available at: http://press-pubs.uchicago.edu/founders/documents/v1ch18s35.html

[2] Omand, D., 2007, 'Reflections on Secret Intelligence' in: Hennessy, P., 2007 (Ed), The New Protective State: Government, Intelligence and Terrorism, London: Continuum Books, pp.99-101. For the purposes of clarity at the outset, it is assumed that interested readers of this thesis will recognise that the 'intelligence' referred to throughout this thesis is that phenomenon, which is conducted in connection with issues of security in its broadest terms, rather than the cognitive processes of the brain in their broadest sense. Of course, the two are not unrelated, or ought not to be!

[3] The specific definition of open source intelligence (OSINT) is also discussed further in Chapter Two (2.4). It is worth stating here that the product derived from the exploitation of open sources of information, where exploitation includes its collection or acquisition, processing, analysis or assessment, and dissemination is understood in much the same way as the product of other intelligence disciplines like Human intelligence (Humint) or signals intelligence (Sigint) is understood. Definitions and taxonomy are discussed throughout Chapter Two. It is also worth noting that, while both the literature and practitioners loosely interchange these terms - OSINT, open source information, and open source exploitation - explicitly in the language they use, the distinctive meanings are implicitly understood.

[4] Cited in US Senate Committee on Armed Services, Hearings on the National Defense Establishment, 1st Session, 1947, pp.525-528, as recounted in Grose, P.,1994, *Gentleman Spy: The Life of Allen Dulles*, New York: Houghton Mifflin Company, p.275.

[5] Discussion with former US Deputy Assistant Director of Central Intelligence for Analysis and Production, CIA, at Oxford Intelligence Group meeting, 5 December 2005. For one useful summary of the various figures quoted from 80 to 95 percent, see also: Bean, H., 2007, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and CounterIntelligence*, 20, 2, pp.240-257.

[6] *Ibid.* Of course the proportion of total resource devoted to open source exploitation would be a much easier figure to derive than its effect. But, that is not the main emphasis of the research effort. Such figures are neither comprehensively stated publicly, nor were they made available to the author. Suffice to say that the author was advised that the UK Defence Intelligence Staff (DIS) budget for the acquisition of open source material (not including labour) amounted to some £300,000 in 2003. By comparison, the total income for BBC Monitoring, which is the UK's largest open source exploitation effort and whose figures are public, amounted to approximately £28m in 2006/07. See: http://www.monitor.bbc.co.uk/review.pdf pp.15-17.

[7] Contemporary intelligence communities are not static entities. Increasingly they now blur once clear lines between, for example, law enforcement and security, between security and defence, between foreign and domestic, and between public and private.

[8] The research has inexorably gravitated towards the UK and US experience, although international organisations are represented. This is partly due to the relatively higher effort devoted to the intelligence function within these countries, partly due to the richer quality and higher quantity of data sources, partly due to the relatively higher combination of closed and open exploitation that allows for their comparison, partly due to the author's own familiarity, partly due to language constraints and partly due to ease of access.

[9] Bean, H., 2007, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and CounterIntelligence*, 20, 2, pp.240-257.

[10] Silverman, D., 2004, *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*, London: Sage.

[11] These are mid 2004 figures based upon interviews and discussion with representatives of all these OSINT cells. By 2007, the resource and budget of these and similar organisations were acknowledged to be increasing incrementally as noted in an interview with the UK OSJWG on 28 March 2007.

[12] This is a mid-2006 figure. The US Asian Studies Detachment, discussed in detail in Chapter Four (4.3), resides outside the closed intelligence community.

[13] Steele, R.D., 2001, *On Intelligence: Spies and Secrecy in an Open World*, OSS International Press (self-published); Politi, A., 2003, 'The Citizen as "Intelligence Minuteman"', *International Journal of Intelligence and CounterIntelligence*, 16, pp.34-38.

[14] I am grateful to Michael Herman for pointing out that little comparison between national intelligence systems has been made. This is reflected and supported in Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press, pp.35-38.

[15] Deibert, R.J., 2003, 'Deep Probe: The Evolution of Network Intelligence', *Intelligence and National Security*, 18, 4, pp.175-193.

[16] However, it is international in the sense that OSINT is practised by multi-national organisations such as NATO, the EU, OSCE, the UN, EUROPOL and ICTY, who do not possess closed source collection capability in their own right but rely heavily for their closed intelligence on developed nation contributors.

[17] Odom, W., 2003, *Fixing Intelligence for a more Secure America*, New Haven: Yale.

[18] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[19] These include, with varying degrees of contact: Infosphere, Exclusive Analysis, 'Political Risk Associates', and Hazard Management Solutions (HMS).

[20] NATO, ICTY, IAEA, the EU and EUROPOL for example.

[21] These include: representatives from Cabinet Office, serving or retired intelligence practitioners, and serving and retired open source practitioners.

[22] The private information brokerage (PIB) HMS works closely with a variety of UK and US intelligence agencies on intelligence analysis, which exposes them to closed information.

[23] Discussion throughout this research with Mats Björe of Infosphere, formerly an intelligence officer in the Swedish Defence Force, together with similar Dutch and South African contacts suggest that the open source exploitation story is a common experience.

[24] Collis, J., Hussey, R., 2003, *Business Research: A Practical Guide for Undergraduate and Postgraduate Students, (Second Edition)*, New York: Palgrave Macmillan.

[25] Strauss, A., Corbin, J., 1998, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (Second Edition), London: Sage Publications.

[26] Silverman, D., 2004, *op cit.*

[27] Eisenhardt, K. M., 1989, 'Building Theories from Case Study Research', *Academy of Management Review*, 14, 4, pp.532-550.

[28] Silverman, D., 2004, *op cit*.

[29] Van Maanen, J., 1979, 'Reclaiming Qualitative Methods for Organizational Research: A Preface', *ASQ*, pp.520-526.

[30] Collis, J., Hussey, R., 2003, *op cit.*

[31] Glaser, B.B., Strauss, A.L., 1967, *The Discovery of Grounded Theory*, Chicago: Aldine; Van Maanen, J., 1979, *op cit;* Collis, J., Hussey, R., 2003, *op cit.*

[32] Morgan, G., Smircich, L., 1980, 'The Case of Qualitative Research', *Academy of Management Review*, 5, 49, pp.491-500.

[33] Slovic, P., 2000, *The Perception of Risk*, London: Earthscan.

[34] Bean, H., 2007, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and CounterIntelligence*, 20, 2, pp.240-257.

[35] Aldrich, R.J., 2005, 'Setting Priorities in a World of Changing Threats', *NATO Workshop on Intelligence Reform*, St Anthony's College, Oxford.

[36] Gibson, S., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22

[37] Johnston, R., 2005, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, p.66; Maddrell, P., 2007, 'US Intelligence Since 2001', Choices for Western Intelligence: The Security Challenges of the Twenty-First Century, Conference at University of Wales Aberystwyth, 28-30 April 2007, at which Dr Paul Maddrell convincingly argued that we should now recognise and move the characterisation of the contemporary era from 'post Cold War' to 'transnational'.

[38] Hennessy, P., 2007, The New Protective State: Government, Intelligence and Terrorism, London: Continuum Books.

[39] Devji, F., 2005, *Landscapes of the Jihad: Militancy, Morality, Modernity*, London: C. Hurst & Co, pp.1-33.

[40] Rathmell, A., 2002, 'Towards postmodern intelligence', *Intelligence and National Security*, 17, 3, pp.87-104; Held, D., McGrew, A., 2003, *Globalization/Anti-Globalization*, Malden, MA: Polity Press; Furedi, F., 2005, *Politics of Fear*, London: Continuum.

[41] Gill, P., Phythian, M., 2006, *op cit*.

[42] Runciman, D., 2006, *The Politics of Good Intentions: History, Fear and Hypocrisy in the New World Order*, Woodstock: Princeton University Press.

[43] Lowenthal, M.M., 1999, 'Open Source Intelligence: New Myths, New Realities', *Intelligencer*, 10, 1, (February) pp.7-9.

[44] A very useful timeline can be found in Steele, R., 2001, *op cit*, pp.341-350

[45] The IOSWG began with the US, UK, Australia and Canada. It now meets annually, consists of 12 countries and shares product via *opensource.gov;* Public recognition of this development can usefully be pegged to: Steele, R.D., 1996, 'Creating a Smart Nation: Strategy, Policy, Intelligence, and Information', *Government Information Quarterly*, 13, pp.159-173.

[46] Aftergood, S., 1997, Secrecy & Government Bulletin: Federation of American Scientists; Gannon, J. C., 2000, Address to the Washington College of Law at American University Washington DC; Clift, A.D., 2003, 'From Semaphore to Predator: Intelligence in the Internet Era', *Studies in Intelligence*, 47; Dupont, A., 2003, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, 18, pp.15-39; Treverton, G.F., 2003, *op cit*.

[47] Hulnick, A.S., 1999, 'Openness: Being Public About Secret Intelligence', *International Journal of Intelligence and CounterIntelligence*, 12, pp.463-483.

[48] Treverton, G.F., 2003, *op cit*.

[49] Berkowitz, B.D., Goodman, A.E., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press.

[50] Florini, A., 1998, 'The End of Secrecy', *Foreign Policy*, Summer, pp.50-64; Held, D., 2004, *Global Covenant*, London: Polity Press.

[51] Gray, C.S., 2005, *Another Bloody Century: Future Warfare*, London: Weidenfeld & Nicholson.

[52] Witness the entire issue of *Intelligence and National Security*, 18, 4, 2003.

[53] And, as the Director of the UK Defence Academy's Conflict Studies Research Centre has noted in private correspondence with the author: "…an object lesson in how not to use open sources."

[54] Hutton, B. (Lord), 2004, *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly CMG*, Westminster: House of Commons, Report No: HC 247, hereinafter referred to as the 'Hutton Report'.

[55] UK Privy Counsellors, 2004, *Review of Intelligence on Weapons of Mass Destruction* (The Butler Review), House of Commons, HC 898; US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company.

[56] Herman, M., 1996, *Intelligence Power in Peace and War*, Cambridge: Royal Institute of International Affairs.

[57] This is not the first time that a national OSINT capability has been advocated or indeed practised within a national IC. In 1996, Dr Jo Markowitz was charged with establishing the CIA's Community Open Source Program Office.

[58] US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company, p.413.

[59] US House of Representatives/Senate, 108th Congress 2d Session, Conference Report 108, dated 7 December 2004, O:\ARM\ARM04J46.LC, available at: http://www.fas.org/irp/congress/2004_rpt/h108-796.pdf p.48.

[60] A new position created by the US Intelligence Reform and Terrorism Prevention Act of 2004.

[61] US Senate Committee on Governmental Affairs: Intelligence Reform and Terrorism Prevention Act of 2004, 6 December 2004, available at: http://www.fas.org/irp/congress/2004_rpt/s2845-summ.pdf p.9.

[62] Johnson, L.K., 2002, *Bombs, Bugs, Drugs, and Thugs*, New York: New York University Press; Lowenthal, M.M., 2003, *Intelligence: From Secrets to Policy*, Washington: CQ Press; Krizan, L., 1999, *Intelligence Essentials for Everyone*, US Joint Military Intelligence College, Washington DC; Keegan, J., 2003, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, London: Pimlico.

[63] Treverton, G.F., 2003, *op cit*.

[64] Krizan, L., 1999, *op cit.*

[65] Berkowitz, B.D., Goodman, A.E., 2000, *op cit.*

[66] *Ibid*, p.80.

[67] Steele, R.D., 2002, *The New Craft of Intelligence Personal, Public, & Political*, Oakton, Virginia: OSS International Press (self-published).

[68] Private conversation between author and Steele.

[69] Steele, R.D., 2001, *op cit.*

[70] This quote is taken from a Headquarters US Army 'For Official Use Only' document: *US Headquarters Department of the Army, 2006, Open Source Intelligence (FMI 2-22.9)*, released to the public via the Federation of American Scientists in January 2007, available at: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf p.1.2

[71] Steele, R.D., 2001, *op cit.*

[72] Gibson, S.D., 2005, 'In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation', *Risk Management: An International Journal*, 7, 4, pp.23-41.

[73] Despite its frequent use, the origin of this phrase is difficult to determine. Arguably, it is a Quaker concept, which articulates an alternative roll for politics beyond violence, see: http://www.quaker.org/sttp.html

[74] Johnson, L.K., 2002, *op cit*, p.xv; Lowenthal, M.M., 2003, *op cit*, p.6.

[75] Silverman, D., 2004, *op cit.*

CHAPTER TWO

LITERATURE REVIEW: MINDING THE GAP

> "The next information revolution asks, what is the MEANING of information, and what is its PURPOSE? And this is leading rapidly to redefining the tasks to be done with the help of information, and with it, to redefining the institutions that do these tasks."
>
> Peter Drucker, 1998[1]

> "The problem with spies is they only know secrets."
>
> Robert David Steele, 2001[2]

2.0 Introduction

Chapter One introduced the research project. It indicated that the contemporary exploitation of open sources for intelligence purposes has been re-invigorated as a result of the recent information and communication transformation. Yet its contribution has been traduced by anecdotal, albeit experienced, estimates of efficiency rather than any understanding of effectiveness in terms of what it can do. Thus, this research project sets out to explore that contribution more critically, beginning with an examination of the literature that confirms such a gap and the setting of a conceptual framework for this project.

First, this chapter looks at the literature on the broader phenomenon of intelligence: its definitions, categories, models and frameworks, which form the context for open source exploitation. Second, this chapter examines three key influences that shape the context of intelligence: globalisation; risk society; and changing societal expectation. This context, which intelligence endeavours to understand, has undoubtedly changed since the collapse of communism in the early 1990s. Yet, more significantly, it notes the ubiquitous influence of the contemporary transformation in information and communication technology (ICT) on all three. It begins to make connections between these key influences, today's heightened status of open source exploitation that reflects them, and the potential implications for the future conduct of intelligence. Third, intelligence, and the contextual influences upon it, are circumscribed by examination of the debate characterised in intelligence circles as 'intelligence reform'. Specifically, it

notes the contemporary 'tactical' situation post 9/11 and post Iraq 2003. These two events, above all, have driven today's intelligence community to examine itself, and to be examined, under the guise of 'intelligence failure'; perennial grounds for examination. Pearl Harbour, Korea, the Falklands War, and the fall of the Berlin Wall, amongst a host of other political dénouement, did much the same in their day. It also notes the return of a 'season of inquiry' into western intelligence communities post 9/11 and Iraq 2003 that has sought to apportion 'blame' for any such failure and attempt correction for the future through legislation, oversight, and wise council.[3] In all of this contemporary debate on reform, several sacred cows are being challenged: a definition of intelligence that prescribes secrecy and proscribes openness; an intelligence cycle that neglects the randomness and non-linearity of networks; and a series of critical distinctions permeating the intelligence debate - nature versus character, risk versus uncertainty, and reality versus perception - that are poorly understood.

Finally, the literature pertinent to open source exploitation, including the little that specifically describes its contribution, is explored in detail. This literature comes in two flavours: 'sparse-objective' or 'idiosyncratic-voluminous'. The idiosyncratic variety is that canon of practitioner work largely advanced by Robert Steele.[4] It reads like a manifesto for root and branch reform of the intelligence function, if not its wholesale dissolution and resurrection in the private sector. Notwithstanding its rhetorical vigour, it is perceived by many to eclipse more than elucidate the substance of its message. It will doubtless remain a significant canon of work, and it has influenced this research, but it does not coherently describe how open source exploitation fundamentally contributes. The sparse variety, generally academic, mentions open source exploitation in passing, more often as part of a broader look at the intelligence function, less often as a discrete subject, and rarely in terms of its contribution to intelligence.[5] It is generally favourable towards open source and invariably recommends that more use should be made of it. The recent spate of intelligence inquiries replicates the literature in this regard. A very few efforts, three of note, generate some objective understanding as to why open source is effective, and how it might be described as contributing.[6] These are taken as a useful start-point for the remainder of this research; but they are still brief and dissimilar. Thus, the gap in

knowledge concerning the contribution of open source exploitation to the intelligence function is significant, both in terms of any research effort at all and the congruity of that which exists. This research fills that gap.

2.1 Intelligence as context for open source exploitation

Rischard has argued that contemporary institutions of government, mired by bureaucracy and left standing by the pace of globalisation, are doomed to irrelevance.[7] Weller has observed that intelligence agencies are no more than bureaucratic structures operating within the context of the civil service of their respective nations: living by rules and functioning by committee.[8] The exploitation of open sources of information within a government's intelligence machinery has been identified as one opportunity to put government back on track.[9]

In order that the national intelligence machinery can optimally utilise OSINT, it must establish OSINT's correct treatment and place within intelligence. However, the literature, while recognising the significance of OSINT, reveals by omission no clear direction for its utilisation. Equally, any change in the conduct of intelligence as a consequence of the formal exploitation of OSINT is barely recorded.[10] Thus, we have a relatively new phenomenon formally incorporated into an established process, whose contribution and direction is unclear to practitioners, and barely understood by any research community. The scarcity of research literature articulates the need for an examination of the reality of the claims made for OSINT. These claims might usefully be examined in an empirically qualitative manner, rather than a hitherto anecdotal one. Understanding the exploitation of OSINT in the intelligence context might usefully reflect the changing conduct of intelligence as a result of that exploitation. In order to understand the claims made for the exploitation of OSINT within the broader context of the intelligence function, it is necessary to examine the literature's view of that relationship by first deriving some understanding of intelligence.

2.1.1 Intelligence: Definitions and taxonomies expanded

> "… all attempts to develop ambitious theories of intelligence have failed."
> Walter Laqueur, 1985[11]

Definitions of intelligence

The literature suggests that a definition of intelligence has been and remains a matter of intractable debate. Scholars, students, practitioners, and consumers of intelligence will recognise a variety of themes that seem common in any such attempt to derive a universal, standard, definition of intelligence: support to decision-making and policy formulation through the production and dissemination of information; the result of analysis; an attempt to predict or foretell events to come - foreknowledge; conducted by nation-state machineries in a clandestine manner; focused on 'foreigners'; as both product and process.[12] In a recent addition to the debate Gill and Phythian note that Intelligence agencies, governmental inquiries, Commissions, legislative bodies, and Acts of parliaments have all attempted the feat.[13]

Warner is credited with an authoritative and classical definition of intelligence. In 2002, he assailed the contumacy of the argument and neatly summarised the effort as:[14]

> "Intelligence is secret, state activity to understand or influence foreign entities."[15]

He demonstrates that all the relevant and diverse themes can be represented in this definition. Furthermore, he supports the argument elsewhere with the writings attributed to Sun Tzu. Sun Tzu's *Sunzi Bingfa*, in which Master Sun extols the virtue of the 'divine skein', or secret web, by which foreknowledge of one's enemy is attained, lends the weight of history and continuity to Warner's definition of intelligence.[16]

However, it is unlikely that Warner can claim to have settled the discussion just yet. Gill and Phythian in their examination of intelligence theory contest Warner for elevating the notion of secrecy while blurring the sense of purpose. They add two aims in order to clarify and endow Warner's 'understand' and 'influence' with objective:

"Intelligence is … aimed at maintaining or enhancing relative security … that allows for the timely implementation of a preventative policy or strategy …".[17]

Equally, recent literature debating intelligence reform articulates the view that Warner's classic definition is not entirely sufficient for contemporary society. For example, Rob Johnston suggests three broadly equal customers of intelligence today: law enforcement; security organisations; and the military, pointing out that their combined adversaries are no longer exclusively foreign entities or concentrated at nation-state level. Thus he modifies Warner's classic definition to: "Intelligence is secret state or group activity to understand or influence foreign or ***domestic*** entities."[18] He has added the domestic arena and implied something beyond the state conducting it.

Keegan's definition of 'real-time' or operational intelligence broadens the scope still further: "Who knows what in sufficient time to make use of the news …".[19] He goes on to distinguish operational intelligence, essentially predicated upon communication means, from espionage, which characterises strategic intelligence and broadly outside the 'range' of operational intelligence. The definition is shifting to one that might more accurately reflect contemporary intelligence activity as simply support to decision-making.

Who constitutes the intelligence community is also being modified. In contemporary western societies, security is no longer the preserve or concern of the public sector or state. The private sector bears a significant proportion of the burden of contemporary security risk, both as target and response. Not surprisingly, it is steadily building capacity to manage it, and part of that capacity is an information input, which this research demonstrates in Chapter Four (see 4.2.2-5 in particular).

Additionally, secret state activity, as conducted by a 'national' intelligence community, has never been the only means by which to understand and influence. Open sources of information inside and outside secret state activity, diplomacy and the media respectively, have long been powerful informers.[20] Furthermore, these sources are also available to inform those who conduct a closed effort. Thus, Warner's definition and

amendments to it fail to capture the complete information business that supports decision and policymaking across the entire security and risk management spectrum. What Warner's definition does do is articulate and 'split-out' the more precise role of spying or espionage, as in secret intelligence, within a national intelligence and security community. The clandestine remains a thoroughly legitimate endeavour, but it is not the entire gamut of the information business or even intelligence.[21]

Omand perfectly encapsulates the dilemma of a definition of intelligence, when he suggests that: "the ultimate object of intelligence is to enable action to be optimized by reducing ignorance; and of secret intelligence to achieve this objective in respect of information that others wish to remain hidden."[22] In highlighting the 'secret', he neither rules in, nor rules out, the possibility of something other than secret intelligence contributing to that optimisation of action. Furthermore, and hinting strongly at what that other might be, he goes on to say that open sources are important and increasingly so for the intelligence community.[23] Thus, the ingredient of secrecy remains simultaneously crucial to and controversial in any definition of intelligence, and is explored further throughout this thesis. With a nod to Keegan's pragmatic definition, Omand's subtle observation, and supported by the contemporary formal inclusion of open source exploitation within intelligence communities that this research details, the author's own working definition of intelligence is put simply:

> "Support to decision-making."

Taxonomies of Intelligence

Setting aside the discussion on the contemporary relevance of Warner's classic definition of intelligence, there are numerous ways of categorising the intelligence function that expand the 'why' and 'how' of intelligence:

- Historically, differentiation by geographical region has been a standard compartmentalisation. Nation state intelligence agencies have taken large swathes

of the world; Russia (especially as Soviet Union) to the Middle East, the Far East, Latin America *et cetera* as the focus for their activity.

- More recently and certainly post WWII, a differentiation has emerged based upon threat category; military, criminal, terrorist, weapons proliferation and narcotics for example. Post 9/11, the emphasis on counter-terrorism has become prominent.
- Herman succinctly divides intelligence into function, activity, product and process as he traces its creation from input to output.[24]
- Odom further articulates the division as that between 'collection' of information and 'analysis' of that information.[25]
- Treverton stresses the distinction between intelligence as evidence necessary to stand up in a court of law, versus intelligence as security of a nation-state, which may never see the light of day.[26] The historical distinction between law-enforcement intelligence as evidence on the one hand and military and national intelligence as predictive analysis on the other is a significant taxonomy. The need to bring people to justice through the courts using admissible evidence is proving difficult to rationalise against the imperative for intelligence security. This difficulty is more developed in the US than the UK; Guantanamo Bay and 'detention without trial' in Bellmarsh Prison respectively. Furthermore, the rivalry between the CIA, the DoD and the FBI that in part emanates from this distinction, is well documented and contributes to the competitive culture in which intelligence is conducted.[27] Indeed the very creations of the Director of Central Intelligence in 1947, the US Department of Homeland Defence in 2002, and the Director of National Intelligence (DNI) in 2004/05 were responses to such rivalry. Similar rivalries have been experienced in the UK. The author, for example, experienced the 'competition' between law enforcement and intelligence agencies in Northern Ireland throughout the 1980s and 1990s.
- Both Herman and Bruneau distinguish intelligence by its practitioners.[28] Although intelligence is a largely British-European invention that has been exported around the world, its employment has either been as a tool of the state to support decision-making or as an instrument of the state to enforce its decision-making.[29] The use of intelligence in the Soviet Union, for example, set the tone for the latter. Herman

further describes this useful distinction as being between the 'western' model and 'the rest'.[30]

- Shulsky and Schmitt identify the key agencies or sources involved as being a useful taxonomy: Human Intelligence (Humint); Technical Intelligence (Techint), which itself includes Signals Intelligence (Sigint), Imagery Intelligence (Imint), Measures and Signatures Intelligence (Masint); and finally Open Source Intelligence (OSINT).[31]
- The custodians of the most expensive intelligence capability, the US, divide their intelligence operation into collection, analysis, covert action and counterintelligence.[32] Together with other exemplars of the western model they would also recognise the scope of intelligence as being: national security (as in foreign), domestic or internal to the nation, law enforcement and economic corresponding to Johnston's analysis above[33]
- The level and purpose for which intelligence is conducted might also be distinguished as strategic, operational, tactical and technical for broad management purposes.

All these taxonomies have their value, each of them is valid, and of course all of them are practised simultaneously, whether they are the taxonomy in vogue or whether they reflect resource available. However, most of these taxonomies focus on mechanism or organisation rather than purpose or outcome. This thesis is not so much concerned with taxonomy other than to note that such a variety contributes to compartmentalisation, which is often justified on the grounds of security. This compartmentalisation, and its bearing upon security and secrecy, contributes to the culture in which intelligence is conducted. It cannot be ignored in any serious study of intelligence activity and is returned to throughout the thesis.

However, security and secrecy are often improperly connoted for each other or simply interchanged. Hulnick argues that:

> "Intelligence agencies have a tendency not to share particularly sensitive intelligence data with their counterparts in order to protect sources and methods, to be sure, but sometimes they withhold data because having the

> sensitive material gives them power and the ability to one-up the other agencies. It sounds childish, but it is a fact of life."[34]

Furthermore the varieties of intelligence conducted create significant demand and competition for resource. This leads to budget protection and 'turf-wars', which only serve to enhance compartmentalisation. When added to the needs of security, it reinforces a rigorous culture of secrecy in which intelligence is conducted.

The purpose and outcome of intelligence is of much greater interest. The literature is deficient in discussing how intelligence, as a secret state activity, can speak to and demonstrate the objectives of, a nation-state. However, the literature on security sector reform, particularly in developing countries, is beginning to trace a different role for intelligence.[35] In terms of telling truth to power, the most meaningful outcome of the intelligence function in this arena is in creating the possibility to place trust in others by those who have to place it. In a developing nation's early years the implication is that this is a one-way process between the state and threats to the state.[36] Perhaps in developed states this process is equally applicable to the relationship between the state and its own citizens.

As ever-wider uses for intelligence are being shaped in terms of telling truth to power, it would be wise to retain an understanding of what is meant by truth. Without disappearing down a philosophical rabbit hole, Dr David Young's version - the founder of Oxford Analytica - is worth remembering: "Truth is what conforms to reality".[37] Yet, knowing what is real involves placing trust, to a large degree in the absence of certainty, thus placing trust is itself about taking risk and ultimately, a leap of faith.

2.1.2 Intelligence models

> "Any theory of strategic intelligence must be built around the so-called intelligence cycle…".
>
> Loch Johnson, 2003.[38]

In addition to the intelligence taxonomies that essentially reflect the collection targets and systemic processes of intelligence, the literature survey shows that there are three models pertinent to the conduct of intelligence:

- The extant model of the intelligence function as process and known universally as the 'Intelligence Cycle'.
- The stakeholder model of parties involved in the intelligence function as both producers and customers known as the 'Intelligence Commons' model.
- An emerging model of intelligence, recognising a more realistic intelligence process engaged in the 'total information business' across society, which the author has labelled here as the 'network-centric model'.

The 'Intelligence Cycle'

> "Yet it is not a particularly good model, since the cyclical pattern does not describe what really happens."
>
> Arthur S. Hulnick, 2007.[39]

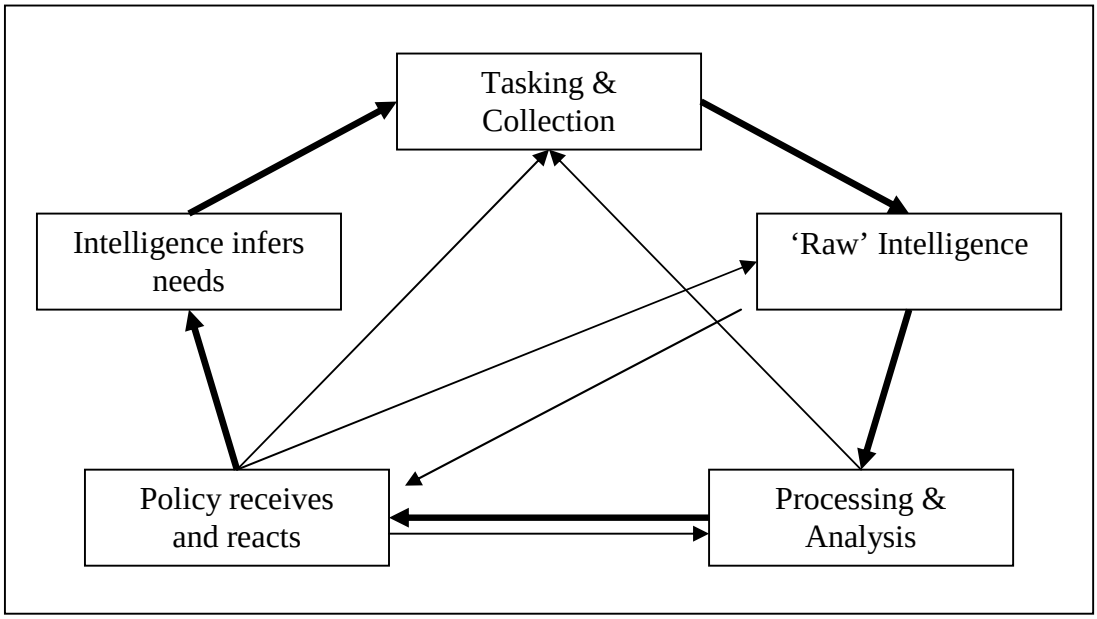
The 'intelligence cycle' has come to be the *de-facto* model for the conduct of intelligence within agencies, across disciplines and by individuals. It is a long established model that has remained consistent through time and commonly used across countries, cultures and organisations.[40] It is not particularly exclusive to intelligence. It is represented by many 'production' cycles across a variety of walks of life from manufacturing to research, the most basic of which might be the 'plan, do, and review' model. This traditional model of the intelligence process, agreed almost unanimously by contributors to the literature, consists of the following sequential steps: Requirements; plan and task; collection; collation and processing; all-source and single-source analysis; production; dissemination; and feedback.

Furthermore, this model is traditionally presented in a circle to represent the production flow initiated by the 'customer' at the requirements stage, through process and production undertaken by the intelligence community, and back to the customer, who either closes the loop or feeds back into the cycle with modified requirements (see

Figure 1.2).[41] This circular flow is taken to represent a process that is dynamic and iterative. It certainly represents a very strong stake in the ground for the intelligence community; rigorously defended and almost intuitively understood and accepted.

Recently, however, the model has come under intense scrutiny from a number of intelligence professionals and academics, and increasingly being questioned for its contemporary practice and relevance.[42] Treverton has developed the 'real intelligence cycle' (see Figure 2.1), and Johnston has developed the 'systems model of the intelligence cycle'; both of which attempt to record the reality rather than the perception of how intelligence is conducted referred to in Chapter One.[43]

Figure 2.1: Treverton's 'Real' Intelligence Cycle



Source: Treverton[44]

Treverton and Johnston jointly sum up the counter-argument when they suggest that the intelligence cycle model reduces a complex iterative process to a linear information-handling map with crucial deficiencies:[45]

- "(It) assumes the process works the same way for all objectives, regardless of complexity and cognitive demands.
- (It) does not represent the iterative nature of the process required for meeting objectives.

- (It) does not identify responsibilities for completing steps and allows for misconceptions in this regard.
- (It) does not accurately represent the impact of resource availability on analysts."

There are other difficulties for the so-called circular nature of the conventional intelligence cycle:

- Intelligence practitioners themselves acknowledge that the circular logic is not always rigorously adopted in practice; short-circuits are formed, when and where it is considered expedient.[46]
- Intelligence 'reformers' argue that, as a generalisable model, it needs to change and adapt to the asymmetric and networked world that it is trying to predict.[47]
- Intelligence agencies know that by the time they have responded to requirements policy-makers have moved on to other issues.
- Policy-makers do not always know themselves what requirements they should be setting among the myriad of crises that cross their desks every day.
- Some US and UK commentators argue that requirements-driven intelligence alone fails to recognise that serendipity plays an important part in 'horizon-scanning' and 'refreshing' the risk-register.[48]

Such is the mismatch that in 2004 the US DoD ditched the term intelligence cycle in favour of 'intelligence process'; recognising all the steps but not the logic.[49] Indeed, in the same document the US Joint Chiefs do not define intelligence until the glossary, while countenancing in the introduction that it does not have to include analysis.[50] This contradiction typifies the confusion and is completely at odds with the literature, which considers analysis the jewel in the intelligence process.

The 'Intelligence Commons'

Steele originated the phrase 'intelligence commons' to represent an intelligence 'fellowship' based upon key groupings in an open networked global society that might mutually contribute to and benefit from the exploitation of intelligence, specifically

OSINT.[51] He sees little need to modify the 'intelligence cycle' model as process, rather the inputs to it (OSINT being the principle one), the participants in it, and the culture in which it is conducted.

The entities that make up Steele's 'intelligence commons' or 'seven tribes' model are: National as in government; military; law enforcement; academic; non-governmental organisation (NGO) including the media; business; and religious. The model was deliberately designed with OSINT in mind, reflecting the more fulsome definition of intelligence as understood by intelligence reformers. As a model for the conduct of intelligence it is based upon an interaction between these seven tribes to foster greater cooperation and sharing amongst all producers and possessors of knowledge. He advocates that OSINT in particular can facilitate this because of its open and thus communicable nature. He further advocates the setting up of global regions of cooperation coordinated by leading regional powers based upon this model.[52]

The significance of this model, and variants of it, lies in its advocacy of OSINT as the *lingua franca*. Precisely because the information is derived openly it is theoretically more easily shared. Steele has certainly raised the profile of OSINT, in the US if not globally. However, the model does not yet exist in practice. It seems unlikely that it will ever exist in its global form given the cultural, economic and political barriers that currently maintain the primacy of nation-states with regard to intelligence. Furthermore, the presence of the most perfect 'all-seeing', 'all-sharing' information system does not mean that contributors will populate it. It is not the communicability or openness of information that is at issue, rather whether one nation trusts another with its information. To this extent it is bi-lateral rather than multi-lateral information sharing that is the norm.

This is not to say that the benefit of sharing is valued less than the detriment of breaching security; but, it is to recognise the human aspects of decision-making. Sharing often occurs outside the closed loops of information security and in less formal ways: from cooperation between individuals at the most finite of tactical levels,[53] through individual groupings across borders as exemplified by transnational civil

society organisations,[54] to deliberate information operations between intelligence communities and the press.[55]

Both the UK and US intelligence communities recognise an imperative to share intelligence. Since 9/11, perhaps more insistently in the US, sharing has become the holy grail of its intelligence community, pursued as much through virtual technical networks as real consolidations.[56] In the UK, the much-publicised models of cooperation - the Joint Terrorism Analysis Centre (JTAC) and the Serious Organised Crime Agency (SOCA) - exemplify a real rather than virtual sharing environment; but it still resembles cooperation confined to security, law enforcement and defence organisations rather than Steele's wider intelligence commons. Whether real or virtual, US or UK, there remains a relatively minor role for open source exploitation compared to closed. Conversely, and more internationally, in the US CENTCOM's Coalition Intelligence Centre, which was established in 2003 and represents some 93 nations contributing and participating in counter-terrorism intelligence, open source intelligence is very much the *lingua franca* precisely because the difficulties of sharing closed are too onerous. A very promising example of the intelligence commons and open source exploitation combined is the creation in April 2006 of the UK's Child Exploitation and Online Protection Centre, which has a staff comprising police, ICT specialists, and child welfare specialists.[57] Their activity is almost exclusively dedicated to the Internet - by implication an almost entirely open source operation albeit covertly conducted.

Part of the reason for sharing, or not, lies in how trust is established and maintained. Trust is a personal exchange optimally conducted by two individuals at most.[58] Each has to place trust based upon the other's trustworthiness or potential to be trusted.[59] These two individuals may represent broader institutions and even nation-states but it comes down to individuals in the long run. This is why bi-lateral arrangements for the sharing of intelligence are the most easily arranged and maintained.[60] Such bi-lateral arrangements can be stitched together to create wider multi-lateral arrangements but the trust and information exchange dissipates accordingly.

Thus, Steele's model assumes too great a role for trust in these cross-cultural, multi-participant relationships. The practice struggles to match the rhetoric. His model is simply too idealistic, and somewhat removed from the practical necessities of existing organisations with long histories and established management structures. They do not themselves advocate revolutionary change and probably do not need it. Rather, they recognise an evolution in the conduct of intelligence affairs.[61] Steele's pursuit of a virtual and virtuous intelligence community, however desirable, is probably prescient, ambitious, proscribed and naïve in the contemporary environment. He fails to recognise the instrumental Faustian or Kantian pact that necessitates compromise between enlightenment principles and bureaucratic institutional systems. Furthermore his model, centred on the national, grates with the developing pattern of globalisation that sees nation-states as only one element in the system of global governance. Emulating the criticism of Sardar and Davies, he takes it for granted that these US-centric ideas are the only ones out there, when other cultures may have generated different notions.[62] As O'Hara points out: social, political, economic and philosophical changes associated with globalisation are altering the conditions for placing trust.[63] The autonomy or isolation of 'horizontal relationships' together with the illegitimacy of 'vertical relationships' has meant that the placing of trust remains problematic and mysterious.[64] It is not more trust that is required but more ways of placing appropriate trust. OSINT may be such a vehicle, but not yet in Steele's utopian format.

In contrast to Steele, globalisation literature identifies four generic participants in the 'global commons':[65]

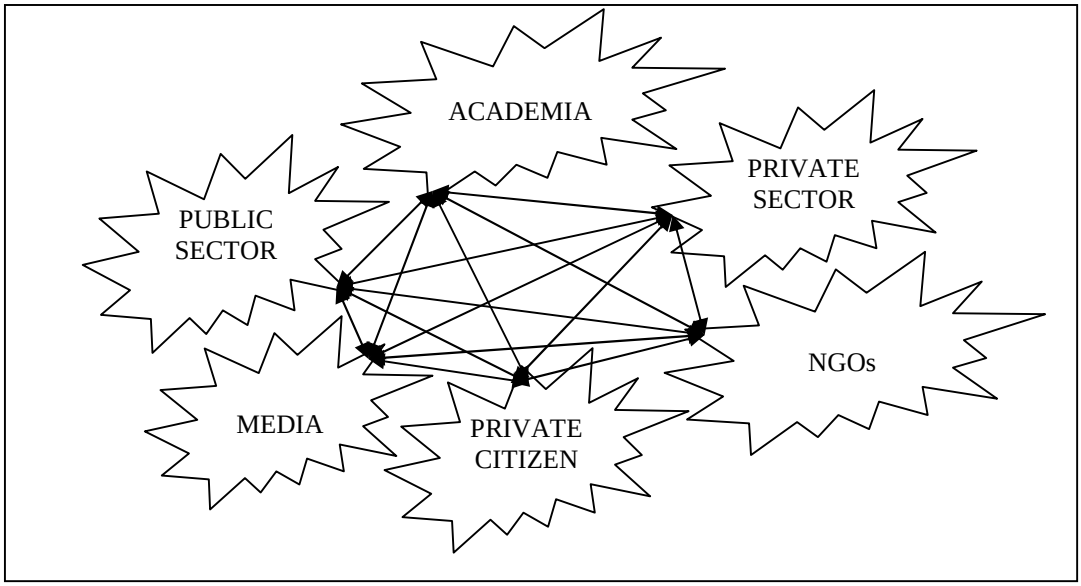
- Nation-state governments.
- Intergovernmental organisations (INGOs) such as NATO, the World Bank, the EU, and the UN Security Council, who comprise representation from individual nation-states but do not act entirely autonomously and certainly not without consent of their constituent nation-state members. They tend to engage problems of a nation-state or perhaps regional character rather than truly transnational. The mixed record of their impact has largely stemmed from the high degree of influence and

vested interests of key constituent member nation-states within these organisations.[66]

- Multi-national corporations (MNCs) such as Ford, Shell or Microsoft who have global presence, an international composition such that it is difficult beyond their headquarters to genuinely identify them with a single nation-state, and generally act autonomously in the pursuit of profit-based goals.
- Non-government organisations (NGOs) or transnational civil society organisations (TCSOs) that organise across nation-state boundaries in the pursuit of their goals. These might be single-issue organisations such as the coalition against land-mines, through single function organisations such as the International Criminal Court, to multiple-issue organisations coordinated as departments by the UN, and religious movements. These organisations tend to have a much greater degree of autonomy from the nation-states they represent than INGOs. They tend to engage more in regional and truly trans-national issues. The mixed record of their impact has largely stemmed from their objectives being at odds with, or of little importance to, key constituent member nation-states.

The author suggests that Figure 2.2 below usefully models the important constituents of any intelligence commons and, by implication, security commons, if not decision-making commons. All of these participants have something to contribute to decision-making, but perhaps absent of the fixed and bureaucratic architecture that Steele seems to envisage, or at least not without some understanding of how networks of trust are established as an intervening step. Because of the contemporary change in ICT, the role of the private citizen is increasingly influential, although whether it is entirely beneficial is discussed further in Chapter Five.

Figure 2.2: The 'Intelligence Commons' revised



Source: Author

The 'Network-Centric' model

Curiously, many of the 'failures' of intelligence to predict or prevent events; Pearl Harbour, the 1982 Argentinean invasion of the Falklands Islands, the 1998 Indian nuclear missile test, '9/11' and Madrid 2004 can be traced back to a lack of effective communication and cooperation between the responsible organisations.[67]

These large impact events have traditionally resulted in significant political efforts to centralise and unify intelligence agencies lamenting (too late) the lack of inter-agency cooperation and intelligence sharing.[68] Pearl Harbour catalysed the 'central' aspect through the formation of the CIA. '9/11' resulted in the formation of the US Department for Homeland Security, the UK's Joint Terrorism Analysis Centre (JTAC) and the creation of an all-powerful US Director of National Intelligence to truly coordinate, centralise and direct US intelligence. Madrid 2004 resulted in the creation of a Europe-wide counter-terrorist Tsar (ironically the one figure in Russian history not informed about the impending revolution!) and calls for a European 'clearing-house' on all matters terrorism (stopping short of a European FBI-equivalent). However, these are all 'after-the-facts' initiatives conducted when emotion is high and logic is short. It

was noted at a meeting of the Oxford Intelligence Group and the Reuters Foundation that it would be better if 'discussion' on intelligence were to occur in the long quiet days of intelligence rather than during the occasional orgies of chaos.[69]

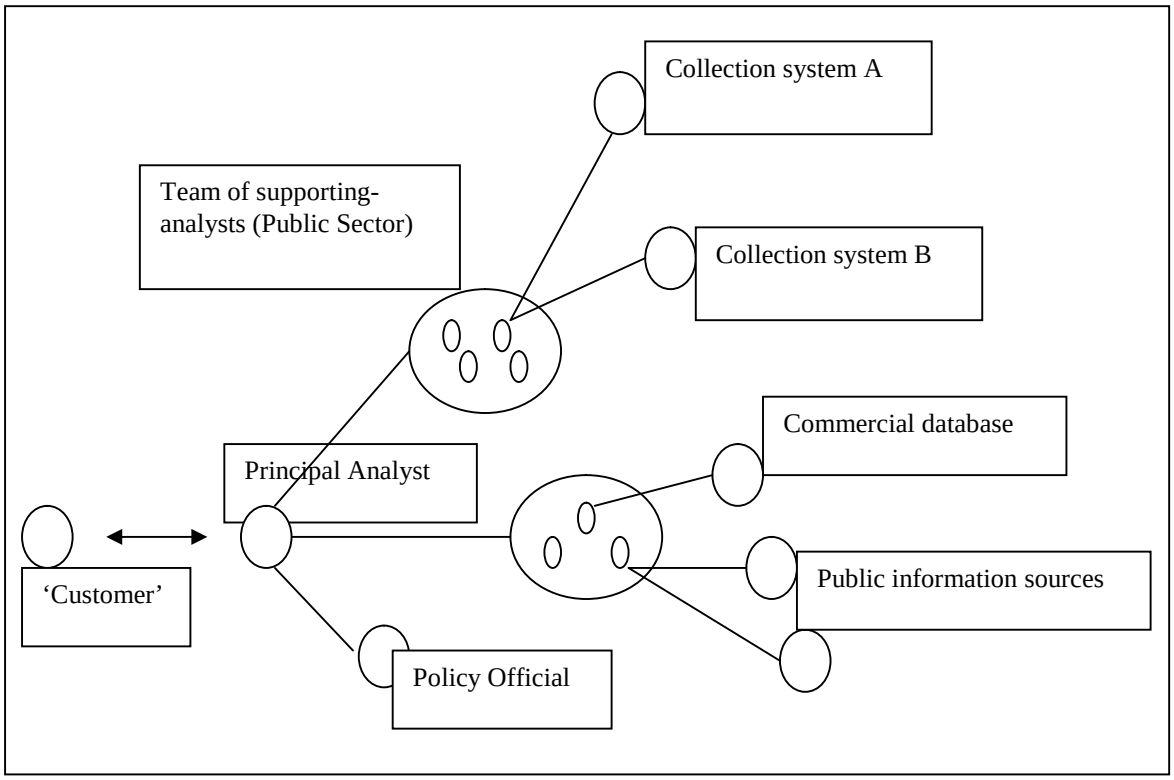
Very little work has been done to understand the context for intelligence on a day-to-day basis let alone future days. While the sentiment behind the urge to centralise and share is understandable it seems that the establishment of yet more agencies that will compete and restrict the flow of information in ever greater bureaucratic creations is questionable. That these organisations are created across nation-state boundaries where cooperation in matters of security, justice, law enforcement, defence, politics, and economics are legally and culturally strained is even more debateable. EUROPOL, for example, already houses a counter-terrorist intelligence-gathering organisation; making calls for a European clearing-house to do the same thing appear rather strange.[70] At best they will merely duplicate their efforts and at worst they will compete.

Berkowitz and Goodman outline the best example of an intelligence reform model encapsulating these dilemmas.[71] They suggest a radically different approach to the 'intelligence cycle' including consumers and sources as integral to the intelligence cycle of the producer. This model reflects a growing unease with intelligence and articulates not just a change in organisation and process but also a fundamental re-think about how and why intelligence is conducted.[72] Recent official attempts to fundamentally rethink intelligence can be found in the July 2004 report of the US '9/11 Commission' and the subsequent US Intelligence Reform and Terrorism Prevention Act of December 2004 creating (among other things) the Director of National Intelligence.[73]

As Berkowitz and Goodman point out, the effect presented by the representation of the 'intelligence cycle' as a flowing circle of efficient information organisation is somewhat illusory.[74] This concurs with Lowenthal's view that the cycle is no more than a linear production line with each action having to wait for the previous action to occur before it can commence its own.[75] Critically, there is little interaction between the producer (analyst) and consumer (customer/decision-taker) from the time of initiation of a requirement to the production of an answer. There is both a geographical and temporal

gap. The validity of such an arrangement in the contemporary fast moving global, ICT, risk environment is suspect. If, implicit in the definition of intelligence is support to decision and policy-makers, then they may not be getting the best support under this arrangement. Thus, Berkowitz and Goodman illustrate a more networked-based arrangement for the process of intelligence that visualises the links between producer and customer to be considerably foreshortened by direct interaction around a central analyst. They call it an example of an intelligence 'virtual team'; based more upon the realistic relationships between participants in contemporary information exchange - networks - than any artificial or idealistic process. Furthermore, it is structured around the notion of a 'principal analyst' at the centre, hence the author's preference for the term 'network-centric' to describe it. See figure 2.3 below.

Figure 2.3: An Alternative 'Network-Centric' Model for the Intelligence Process



Source: Adapted from Berkowitz and Goodman's 'virtual team' model (2000)[76]

In short it unravels the cycle into a linear process, breaks the sequential dependency apart and reorganises the parts into a network with the analyst, at the hub directing intelligence creation. Crucially, it recognises the contribution of OSINT as the 'other

half' of intelligence in addition to the traditional closed. However, it does not suggest how OSINT should be incorporated.

Again, this model does not exist doctrinally, although elements of it are being explored piecemeal and can be observed growing organically now. The model does not wholly explode the intelligence cycle as *de facto* model of the intelligence process. Rather it sits as a half-way house between the intelligence cycle and the intelligence commons models. It recognises that information can neither be wholly owned by organisations nor easily constricted into some sort of uni-directional flow. Thus, it recognises that a wider community of knowledge needs to be engaged on contemporary intelligence subjects. Yet, the process by which the individual elements of that wider community transform data into knowledge largely remains the same. Someone has to set the question, someone has to gather the data and assemble it and someone has to analyse it and produce some meaningful output that reflects the question set.

The direction of this research is most sympathetic to this model. Indeed, all three models have something to contribute to the debate on intelligence reform and the treatment of OSINT with national intelligence machineries. Undoubtedly, a more pragmatic and less utopian variation of the intelligence commons model can be seen in the network-centric model, if one recognises the collaboration of organisations hitherto considered external to the traditional intelligence community. Equally the intelligence cycle can be seen to be alive and well; but, just like the molecular versus atomic scale, this cycle is now more relevant to individual elements of the process rather than the intelligence community as a whole. Why is this happening? Because open sources of information are increasingly available to everyone such that the control and integrity of that information is preserved and generated at the lowest common denominator rather than at the institutional level.

2.2 Forces of change

> "Three things are needed for government: weapons, food and trust. If a ruler cannot hold on to all three, he should give up the weapons first and the food next. Trust should be guarded to the end: without trust we cannot stand."
>
> Confucius.[77]

However intelligence is defined and categorised, whatever the most appropriate model for its creation, intelligence does not exist in a vacuum. The intelligence community is both subject to contextual influences as well as responsible for understanding their impact upon security. It was suggested in Chapter One that three particular forces influencing the contemporary intelligence environment are important: globalisation; the emergence of a 'risk-society'; and the changing nature of societal expectations. They are underpinned in very large measure by the transformation in ICT and the knowledge that ICT creates and disseminates.

The Achilles' heel of knowledge, and the potential dénouement of any association, relationship, organisation or community, is trust. The US 'Declaration of Independence' in 1776 holds: "That to secure these rights (equality, life, liberty and the pursuit of happiness), Governments are instituted among Men, deriving their just powers from the consent of the governed." Implicit in this lofty ideal is open and accessible government.[78] As Abraham Lincoln put it in 1861: "Let the people know the facts, and the country will be safe."[79] Yet, contemporary notions of openness and transparency do not of themselves generate trust and trustworthiness.[80] They may be traduced as such unless recognised for what they are: instrumental means by which to achieve more value-laden objectives, alongside trust; such as honesty, justice, privacy, and fairness.[81]

2.2.1 Globalisation

> "The communications revolution is presenting intelligence organizations with a new challenge far beyond that of mass production. Like other enterprises, intelligence now faces competition from directions believed to have been impossible only a few years ago. Intelligence will have to

> remodel its organization, form new associations, tailor or customize its products and question its fundamental missions."
>
> Richard Friedman, 1998[82]

The phenomenon of globalisation, its source, nature, meaning and impact among a variety of other variables has been widely documented.[83] Its meaning is a little more difficult to pin down. There seems to be at least three important features of globalisation: a notion of 'interconnectedness' thanks to the ICT transformation; a notion of the decreasing importance of territory as nation state boundaries become increasingly porous;[84] and a notion of global liberal free market economics. Rischard posits the additional, albeit rather Malthusian, notion of population growth as driver of globalisation.[85] However, he also suggests that, while its planetary impact is increasing, the institutional capacity to manage it is disproportionately stagnant and bereft of complimentary innovation. It seems that rather than being a driver of globalisation it is more a consequence of science and technology as much as science and technology will provide its management. The ICT transformation powering globalisation is most pertinent to this thesis.

Friedman's assertion above is bold. The gist is clear; yet, as Chapter One introduced and Chapter Five discusses further, it confuses the nature of a phenomenon with its character. The fundamental mission of intelligence is unlikely to be changed by his so-called information 'revolution'. Indeed the very word revolution is questionable. We have had so many communications revolutions, not least the invention of the alphabet, the printing press, the telegraph, the railroad, and aviation, that it has become something of an expected normality. They have all had profound influence upon many characteristics of society including intelligence. But, together with the present digital information explosion, they are all eventually absorbed into the overarching necessity of human engagement - politics - along with all the other cultural, contextual and social influences. None of them effect a change in the fundamental nature of politics - the exercise of relative power - just, maybe, the way it is done and why. As Colin Gray points out, there is nothing essentially different in politics conducted at the level of statecraft (the most important kind still) between the 'Melian Dialogue' of 416 BC and

the overtures to Iran made by the US in 2007 AD: if you do not conform, we may force you.[86]

Running with the gist rather then letter of Friedman's statement, the plethora of information openly available in the public domain as a result of the transformation in ICT has certainly transformed the exploitation of OSINT from being a can-do to a must-do activity, as this research will show. Friedman argues that the ICT transformation is stimulating a 'revolution in intelligence affairs'.[87] Like Drucker he suggests that the present day combination of information and its communication is forcing organisational structure to change of necessity. However, in keeping with the absence of literature on OSINT he does not articulate how the specific exploitation of open sources of information is contributing to that change. Furthermore, he was the unfortunate victim of timing. Post 9/11, one is more likely to be interested in a revolution in the attitude ***towards*** intelligence than in its affairs. Indeed, as discussed later, the perceived discrediting of intelligence in the contemporary period is of itself a reason for the emergence of open source exploitation as a potential route to the restoration of it.

As a result of the changing nature of ICT, we all have increasing access to information sources, which in turn contribute to a more 'aware' if not politicised public. Balancing and managing the expectations of society in an increasingly transparent information environment is often portrayed to be somewhat at odds with a closed intelligence capability. For example, the UK's Freedom of Information Act (FOIA) 2000 is testing that balance,[88] although, the state's ability to resist the spirit underpinning freedom of information legislation is already being observed.[89] Interestingly, the much older US Freedom of Information Act (revised 1996)[90] has, to date, failed to reveal even a broad figure for the US intelligence budget despite the ongoing lawsuit taken out in 2001.[91] However, in November 2005, the newly appointed Deputy Director of National Intelligence revealed a figure of $44Bn for the combined intelligence community budget at a speech in San Antonio.[92]

The transformation in ICT, represented most vividly by the Internet and the personal computer (PC), can also be exquisitely (but perhaps not coincidentally) timed to

coincide with that significant geo-political and historical marker-post, the fall of the Berlin Wall in 1989.[93] The transformation of formerly 'closed' societies to more open ones began to chip away at the need for secret collection as well as contribute to the openness of information. There is another worthwhile point to be made here that should be borne in mind throughout this discussion and for the foreseeable future. Not all open sources of information are digital, and the means of information communication are not solely via the Internet. Furthermore, the contemporary version of ICT transformation can also be more broadly associated with a reduction in border controls, ease of travel, an increasing media 'reach', as well as an increasing 'opening-up' of formerly closed societies.[94] This broader view of ICT transformation as the essence of present-day globalisation is equally pertinent to intelligence and OSINT in particular.

Thus, globalisation in all its manifestations, but particularly in terms of ICT, both creates and reflects issues that are increasingly outside the scope and remit of nation-state government. Yet, the other entities of global governance do not have the power (TCSOs), the motive (MNCs), or the authority (INGOs) to deal with them[95] without recourse to the wishes of nation-states or increasingly (presently), ***the*** nation-state, the US.[96] Most of these issues are economic, financial, science and technology, or security rooted. All are humanly engineered ranging from accidental through erroneous to deliberate.[97] While TCSOs may not have the power to effect change they have certainly understood that moral authority, based upon transparent knowledge, provides convincing reputational risk management challenges for the other entities (offending in their eyes) within the global commons.[98]

2.2.2 Risk society

> "If the developed world is the paradigm of a 'risk society', risk societies must be characterised simply by their perceptions of and attitudes to risk, and not by the seriousness of the hazards to which people are exposed, or the likelihood that those hazards will harm them …"
>
> Onora O'Neill, 2002.[99]

Advances in science and technology, which in industrial societies were once synonymous with risk-taking and progress, have in contemporary society become associated with uncertainty, fear and risk-avoidance.[100] This fear and uncertainty is perceived, if not actually, to have cancelled out the notion of progress and replaced it with a notion of vulnerability.[101] Indeed, some consider the advances generated by science and technology as now threatening the very nature of our humanity.[102] When combined with the reach of the media, or perhaps because of it, the perceptions of risk created among its consumers vary wildly, and often at odds with 'experts' in the field.[103] This dichotomy of perception versus reality, in societies that have broadly been accustomed to solutions of merely complicated issues rather than coping strategies for complex and ambiguous ones, is as pertinent to intelligence as it is to most other societal institutions.[104]

Risk has become an all-pervasive characteristic of contemporary western society. It has migrated from its original support to financial decision-making - insurance - to percolate through every aspect and every level of organisation, including to misrepresent the value-based notions of 'corporate governance' for instrumental and mechanical ones.[105] Risk in this sense, as distinct from risk management (an emerging discipline that purports to cope with the reality of risk rather than the hypothetical) has become philosophy and ideology, competing with, if not replacing, all previous such incarnations. It has become the leitmotif or standard against which we 'tally' any and all human activity. Yet, its greatest dilemma as discipline is its apparent inability to distinguish risk, the combination of likelihood and outcome based upon data, from uncertainty characterised by randomness and the absence of data. The management of risk has somehow taken on the organisation of uncertainty.[106] In short, like it or not for now, we perceive that we have become a risk society.[107] This may be true, but it is not new, and this is so for intelligence as for many other facets of contemporary society.[108]

How does risk impact upon intelligence? The emergence of a risk-society together with the demise of a single Cold War adversary has resulted in a myriad of challenges now able to vie for the attention of, and management by, nation states. Not all of them can be efficiently addressed through closed intelligence. Indeed, closed intelligence

does not have sufficient resource to address all of them were it appropriate. Here, OSINT is increasingly being utilised to complement closed where appropriate; not just in shedding light upon the reality of risk but also in communicating and thus framing the perception of those risks.

Loch Johnson suggests that alongside three key factors pertinent to a nation-state - its world-view, its affluence and its regard for the value of information - its risk appetite will be crucial in setting its intelligence agenda from the outset.[109] By 2004, the western world had become preoccupied with international terrorism despite our newfound philosophy of risk telling us otherwise.[110] We suspended the realities of global risk prioritisation in terrorism's favour and at our collective peril.[111] This is not to say that terrorism is not a pressing challenge of contemporary society but it does not merit being ***the*** pressing challenge. Indeed, some commentators suggest that security threats are interrelated, and intelligence units that leave risks beyond terrorism to other agencies are missing the point.[112]

Devji takes this point further and suggests that some risks, which we would not ordinarily co-locate in a traditional sense, do indeed have some locus of commonality in their global, 'political' nature. Existential threats as diverse as animal rights, anti-global protest and jihad have emerged almost as an accident of globalisation, absent local victories wherever they manifest, and certainly without a recognisable political intentionality.[113]

Without doubt the greatest risks we face, outside the natural, are those that we engineer for ourselves with respect to the 'pale blue dot' that is presently our environment.[114] Yet the management of those risks, by comparison to the chosen course of action for the management of terrorism (war on an abstract noun[115]), should pale into insignificance by any measure, however crude, that one cares to use - monetary expenditure[116] or deaths accruing.[117]

Risk management is to risk as economics is to wealth creation; it confers methodology on the phenomenon of risk. However, contemporary risk is no longer merely

complicated and resolvable by science like the nuclear power and chemical industries of the 1970s. It has also become uncertain and ambiguous,[118] or as Atlee describes it: 'comple**xx'** (*sic*) with a double 'x' for emphasis.[119] Thus, progressive risk management, like progressive economics, is shedding the established norms of positivist theory for a more phenomenological approach. Ormerod, in his 2005 critique of traditional economic theory, describes economics as the suspension of reality for a moment of equilibrium, all other things being perfect or rational, or in every way not of the real world.[120] Traditional economics has become reductionism of the most deceptive kind; its hold over contemporary thinking so strong that when economic theory deviates from practice, it is the practice that is wrong not the theory.[121]

Positivism in this sense demands solutions, quantifiable outcomes, and mathematical models to theoretically represent reality. Practically, it finds expression in the demand for ever-increasing productivity, efficiency and profit, which proves difficult to sustain, or damaging where it is.[122] Furthermore, the desire to meet performance targets in an effort to be transparent, may serve only to make institutions appear trustworthy as opposed to actually being worthy of trust.[123] It seems that we have jettisoned insight, understanding and judgement, together with a willingness to live with the consequences of uncertainty, in favour of an incredible hubris that leads us to believe that we can predict the randomness and manifestations of such consequences as well.[124] Institutional intervention in matters of complexity, particularly those that have a social construction to them, based upon a positivist approach, flies in the face of an increasing body of research. This research suggests that complex interactions between agents gives rise to future consequences of such uncertainty that planning in order to deter their intended consequences is of limited use.[125]

Two examples will suffice. First, world income inequality, as measured by Maddison and modified by Ormerod using the Gini coefficient, has worsened since 1950 despite the global effort to intervene.[126] Perrucci and Wysong observe a similar downward trend in social mobility among 2,749 American fathers and sons between 1970 and the late 1990s, again despite government intervention.[127] Second, efforts to reduce segregation and promote integration by macro or global intervention fail to dissipate the

very strong tendencies to mix with 'similar' people at a local level. Schelling's model demonstrates that at the individual level, people simply do not feel that strongly about integration - they are happy to integrate; but it just does not happen.[128] In these and many other complex social constructs, we have endeavoured to predict, plan for, and control outcomes. Sometimes policies work; more often they fail. The sheer dimensions, the scale and the complex interacting influences make comprehension let alone control extremely problematic. Systems of this complexity are more random than rational. Uncertainty prevails.

Risk management (absent the strictures of political correctness, gratuitous litigation and jettisoning of common sense that feeds the superficial, charlatan-like treatment of risk), is adopting qualitative understanding and coping strategy as optimum resolution for governance. Modern risk theory suggests that terms like 'closure' and 'solution' are already redundant for 'complexx' (*sic*) risk. They are devoid of a sufficient knowledge base and opportunity for deliberative discourse to be truly solvable; yet, governance, constructed on nation-state government, persists with them.[129]

The closest that literature from the intelligence community gets to incorporating this new conception of risk is Treverton's articulation of new threats as 'threats without threateners', and Dupont's 'new intelligence targets'.[130] However, not all risks are threats in the sense of deliberate, malicious human engagement. Some risks originate in natural disasters and some in accidental hazards; but they all present challenges. In some cases a comparison of their outcomes makes such a semantical debate irrelevant but would perhaps offer greater clarity of priority, if 'benchmarked' according to their risk potential.

In short, risk is the measure by which future challenges can be prioritised. Intelligence has not fully engaged the 'science' and methodology of risk that Johnson considers will help it determine how much spending for spies is deemed necessary.[131] Nor has it been fully engaged in providing risk leadership alongside risk management whereby significant societal debates should attempt to redress the balance between risk-taking and risk-avoidance through encouraging an understanding of risk-acceptance. The

notion of risk, particularly 'risk society' and the confusion of risk with uncertainty, is addressed further in Chapter Five (5.2.2) in the context of its relationship to intelligence. For now, it is sufficient to suggest that the role of OSINT in exposing intelligence to information it would not normally see, and thus prioritising decisions about risk solely upon closed information, might be useful.[132]

It is interesting to note that in many parallel ways, academia and intelligence are experiencing similar 'growing' pains. Academia has perhaps recognised the issue earlier than intelligence. The very emergence of qualitative social science research methodology concepts such as 'action research' and 'case-study', compared to quantitative pure science methodologies like experiment and survey, replicate the debate between 'insight' versus 'measurement', respectively.[133] Nye articulates a parallel conundrum for intelligence when he distinguishes 'puzzle' from 'mystery';[134] terminology that has found resonance in the literature on contemporary challenges for intelligence and contingent intelligence reform.[135] Puzzles have become synonymous with tactical, secret measurement, while mysteries require strategic, sense-making insight. The former are considered solvable, the latter irresolvable. Is it not within the purview of intelligence to utilise both ends of the research spectrum? In a highly complex, interconnected, multi-polar, networked world it is understanding, leadership and coping as much as management-type solution that will help societies and its citizens to engage and coexist in trust.[136]

2.2.3 Changing societal expectation

> "As an ever larger number of nations turn toward the establishment of democratic forms of government with more transparent societies, public sources of intelligence have grown in importance."
>
> Loch Johnson, 2003[137]

The ICT transformation powering globalisation together with risk society, have emerged as two crucial challenges for nation-state governments in the contemporary era.[138] Where they collide and find expression is in the changing nature of societal expectation.[139] The increasing ability of information to be communicated, if not globally as a result of the digital divide, then certainly to interested parties around the

globe, is manifest in an increasing societal interest in matters of risk however negatively constructed. This interest in risk is rapidly interpreted as a question of trust between institutions, and between publics and institutions that govern them.[140]

But, governments, in response to risk, see themselves more and more as being about the delivery of good governance and less and less about the articulation of purpose and the meeting of objectives. Contemporary governance has so absorbed the language of risk that it is not merely the fashionable medium for everyday conversation, but has become internalised as process, permeating everything we do; collectively if not individually.[141] Governance, that which governments 'do' to control and steer organisation, necessitates the implementation of policy that fairly balances politics and economics, within the framework of the law, to deliver social benefit. In turn good governance implies sound decision-taking and policy-making that will distinguish a genuine democracy from a kleptocratic demagoguery and an illusory parliamentary image.[142]

In the economic community the tired debate between business pursued for the maximisation of shareholder value versus business as part of a broader social contract is finding a middle ground, whereby social issues are being built into corporate strategy.[143] On the one hand, increasing exposure to globally significant issues, such as poverty and corruption in Africa, forces business to confront them, and on the other an increasing understanding of risk as reflection of contemporary society encourages corporates to manage it proactively. In 2005, Ian Davis, Managing Director of McKinsey and Company, articulated business's ultimate purpose and the private sector response to changing societal expectation as: "… the efficient provision of goods and services that society wants."[144] Implicit in this message is a negotiation of what that middle ground should look like. The emergence of 'blogging' as an established form of 'society' communicating with commerce is a very real example of changing societal expectation.[145] Indeed, some commercial organisations have adopted the technology to communicate back in order to establish meaningful two-way dialogue.[146]

It is not so much that organising can produce a result greater than the sum of its parts. The industrial revolution demonstrated and cemented that relationship. Rather, it is the

sentiment - why - underpinning the structure of how we are organising ourselves that is changing. Structurally, relationships are increasingly network-centred, often virtual, self-organised, and certainly digitally enabled. Underpinning these network structures though is an almost counter-intuitive notion of informality and chaos, which seems 'different' and interesting. It is not the same nature that is at the heart of so-called network-enabled capability (NEC) or network-centric warfare (NCW). For all their claims they remain essentially hierarchical, controlling and power-based notions that merely purport to emulate the 'hip' and 'streetwise'. The effect of informal chaotic relationships of the genuinely interested and well informed distributes outcomes to where they are required by and for people who are direct agents of them rather than people who sense that they ought to be. These may not be politicians. The traditional forms of communication and power relationships have tended to be one-way. That is to say - we talk, you listen. Again this is a form of command and control albeit disguised as 'modern' or 'contemporary'.

And, it is not just that we are entering a 'new era of conversation' as Scobel and Israel put it,[147] rather, that the ICT transformation is allowing more and more people to rediscover political engagement via a different media. The transformation in ICT is obviously supporting this change; however, there are other powerful forces contributing - political disengagement, social disaggregation, and a cynical disbelief in science.[148]

Thus, changing societal expectation finds a voice in influencing public policy. Again, there is little new in this. The English Civil War, the suffragette movement, and the anti-land mine campaign are forerunners to campaigns of the contemporary information age. However, one might observe that, with the transformation in ICT, both the breadth and depth of the subject matter of these campaigns is increasing. Equally, the subtlety of the pressure applied in contemporary campaigns also speaks to the changing nature of political debate. Pressure groups sense that the application of pressure upon market reputation is a more direct route to achieving their own aims than through the traditional route of government legislation. In this sense they also encompass the worst manifestations of 'risk society'. Protest and pressure groups fully understand that both public and private sectors are easily sensitised to reputational risk.

Thus, globalisation, risk society and changing societal expectations are harnessed in contemporary society as a new manifestation of politics and the shaping of public policy. Whether it is interpreted as 'clever', or 'bullying' or 'just the way it is', this convergence of phenomena creates a vacuum of debate. The loser is politics and democracy in the true sense of those words; examples are legion from animal rights protest to Jihad. These protest and pressure groups all understand and manipulate the convergence of risk society and globalisation to engineer and foster changing societal expectation.[149] In September 2005 a full page advertisement was taken out in *USA Today* by a public interest group called the Campaign for Safe Cosmetics against three leading cosmetics companies urging them to accede to a voluntary code of conduct for an ingredients-testing regime.[150] The classic and sad example in the UK is Huntingdon Life Sciences, an animal scientific research facility, who have been subjected to direct and indirect pressure to cease their activities. The significant element missing in these and many other disagreements is debate itself. The protagonists of vivisection - governments, scientists, industry, and customers - seem terrified and spineless in defending their cause in the face of the enthusiastic nihilism of the protestors. There is no discussion; there is only a politics of fear, where logic is defeated by emotion because it lets it.

More effective responses - risk communication strategies perhaps - in turn rely on sound information, the partial provision of which is an intelligence responsibility. However, if a significant proportion of that information is being generated openly and thus outside the remit of a 'closed-oriented' intelligence community then, unless other steps are taken, only a partial picture will result from the intelligence community. This may indeed be acceptable if the entire picture is put together somewhere; but given that intelligence agencies practice OSINT to varying degrees it seems unlikely. Furthermore, the variation in practice across agencies suggests that the treatment of OSINT remains to be clarified.

These three contemporary paradigms have been articulated because they shape the context in which intelligence has to operate and is itself shaped. In this regard, the three paradigms equally reflect how intelligence is changing; or at least having a debate

with itself about change. Globalisation, rooted in the ICT transformation, presents intelligence communities with new boundaries to set for its own definition, new areas to collect in, new challenges for processing and dissemination, and new targets for their work. Risk has become an all-pervasive discipline that, in a managerial sense at least, attempts efficiency of effort through scientifically prioritising challenges faced by any organisation at any level. Changing societal expectations suggest that there is something beyond merely security, some notion of greater purpose perhaps, that intelligence communities need to factor in at least.

Of the three, changing societal expectation probably presents the most complex driver for intelligence and the debate surrounding intelligence reform. Terms such as 'rights', 'transparency', 'governance', 'accountability' and 'trust' are increasingly pervasive metrics of this paradigm. They are freely used even in discussion of the discipline of intelligence, which by its very nature legitimately demands equal consideration of a degree of security or privacy in order to be effective.

Changing societal expectations concocted in the powerful currents of risk society and made manifest through the transformation in ICT is a potent and heady mixture. On the one hand there are many advocates of this new kind of deliberative yet participative democratic style, arguing convincingly that political activity on a global to local scale will inexorably err towards a universal truth more so than any parliamentary type system, where decisions are taken on our behalf. On the other hand there are those who 'worry' that the optimism, which often accompanies idealism, whilst noble and encouraging to witness, flies in the face of the natural pessimism of historians when it comes to matters of politics and the exercise of relative power. Arguably, certainly from a western point of view, in the pursuit of realism, one would prefer to be pessimistic but wrong than optimistic and wrong.[151] The exercise of Nye's concept of 'soft power' is not to be confused with the powerful being hijacked into pursuing soft ideas.[152]

Interestingly, Colin Gray, having gone to some length to relegate cultural influences on war to a secondary position behind politics (unlike John Keegan, who has it the other

way around), does not dismiss it as a challenge for western societies at least. Yet, in exercising a note of cautious realism, he strays dangerously close to misanthropy.[153]

2.2.4 Trust and the forces of change

It is the author's view that the most important of values is trust. Democracies run on trust.[154] Trust is an intangible phenomenon held in the minds of individuals and organisations; most difficult to gain and quickly lost.[155] However, trust has become synonymous with openness, accountability and transparency, which as has been suggested, do not of themselves engender trust merely by their mechanistic presence.[156]

Whether we live in an age where trust is truly in crisis or just an age whose culture is suspicious and cynical, we sense a need to restore trust, or at least the perception of it. We are increasingly urged to communicate in ways that acknowledge human rights and that are open to assessment, accountability and transparency. However, the passive expectation that rights are due in the absence of, or even in equal measure to, responsibilities, is subverting the active role of citizens to generate trust through the conduct of duty. Accountability that is merely the substitution of meaningful outcomes with positivist measurable targets is not good governance. Openness and transparency that has no care for the integrity of its information or trustworthiness of its informants is not a test of the truth but a perpetuation of (increased) deception. Perhaps, ultimately, the only remedy for a crisis of trust lies in the self-disciplined control of each and every individual action that collectively forms community, society and organisation.[157]

Communication is the oxygen of trust.[158] Yet, meaningful communication relies on an intelligent audience capable of receiving a message that is honest and absent misinformation and disinformation. For now, it is sufficient to at least suggest that OSINT can breach the communication gap created by genuine security concerns, and play a direct role in the creation of more 'appropriate' trust.[159] However, if subjugated to the culture of secrecy, compartmentalisation, and risk management rather than risk leadership, then it will simply become yet another closed source; ironically so, given its title. Letting the people know the facts may very well contribute to Lincoln's informed

consent, particularly in government by the governed;[160] but informed consent has to be placed on some basis. Tests of trustworthiness remain the foundation of democracy.[161] Does OSINT have a role to play in the wider discussion of the contemporary role of intelligence in democracy, whose foundations are constructed on trust? Such a link has been suggested elsewhere by the author, but not proven.[162] It may be too great a link to prove; but this study will certainly address the issue.

2.3 Intelligence reform

> "Whether to reform US intelligence is no longer the question. Responsible leaders and legislators must now cease their bickering and ask, 'What reforms make sense? Will they be effective?'"
>
> William Odom, 2003[163]

The growing influence of the forces of change on intelligence has not gone unnoticed. Yet, so-called 'intelligence failure' probably remains the strongest motivation for intelligence reform, however knee-jerk it sometimes appears to be.[164] At the heart of intelligence failure it is analysis more than collection that receives the blame.[165] Johnston points out that research conducted since the 1930s demonstrates that 'forecasting experts', while performing better than novices and machines, rarely outperform statistical models such as Bayesian distributions. Interestingly there may be two exceptions: first, when the statistical data is given to the analyst, the analyst performs as well as the model; second, when the analyst is provided with privileged information, the analyst can outperform the model.[166] However, the advantage conferred by such privileged information remains only as good as the veracity of that information, and privileged does not necessarily imply secret. Finally, aligned with intelligence failure is usually a lack of cooperation across the intelligence process, a poor targeting priority, an unwillingness by customers to listen, and an inability to form trust with the public that pays the bills and deserves a good product.

The loudest calls for intelligence reform come from the largest intelligence-purchasing nation-state - the US. These calls come from all quarters of US society - practitioners retired and serving, politicians, academics, and private citizens. Intelligence and the

reform question are widely and publicly debated. In 1994, Senator Arlen Specter[167] declared of the CIA: "The place just needs a total overhaul." He added: "We are spending a lot of money on the CIA and there have been doubts for years as to whether we are getting our money's worth."[168] These remarks rather summed up collective American opinion at the time and resulted in the two key studies of an intelligence design for the 21st century.[169] However, he neglected to note that 80 percent of the US intelligence budget goes to the Department of Defense, rather than the CIA, and is fiercely protected by it. The appointment in 2005 of a Director of National Intelligence has done little to change this relationship.

In a sense little has changed either since these studies or indeed since the inception of the CIA back in 1947. Two explanations emerge as to why. First, like other studies previously and subsequently, they encounter a very real difficulty in evaluating the worth of intelligence. Second, partly due to the secretive nature and partly because intelligence is a nation-state asset, intelligence scrutiny ends up being intelligence advocacy.[170] Pressure for reform in the US, with the notable exception of the 9/11 Commission, thus tends to come from outside government.

Calls for reform are aimed at both collection and analysis. The former is considered to be technical-heavy and human-light. That is to say that a disproportionate amount of resource (time, money, labour) is spent on technical intelligence collection, much of which cannot be processed anyway due to sheer volume, and not enough resource is put into human intelligence, where the nature of the terrorist threat really resides. The latter analytical side of the house is also coming under increasing criticism. Treverton sums up Johnston's post-9/11 ethnographic study of the 'downside' of the US analytic community thus:[171]

- There is no standard analytic method.
- Analysis serves to confirm pre-existing views.
- Data is not always validated.
- The analytical culture is risk-averse and heavily bureaucratic.
- The analytic culture emphasises error-avoidance rather than imagining surprises.

- The process is dominated and driven by current intelligence - 'CNN plus secrets'.[172]
- Analysts report rather than analyse.

In short analysis is driven by the analysts rather than any strategic agency or government objectives.

By contrast, the UK experience has broadly been to avoid wide and public discussion of intelligence reform other than in times of 'intelligence chaos'. Rather, such discussion does tend to occur in 'quiet' times among the cognoscenti of well informed, discrete circles including the respective UK Parliamentary intelligence committees.[173] Again, to the UK's credit, limited public debate or not, public action is taken. The creation of JTAC and SOCA are examples of real reform, rather than virtual inter-agency cooperation and information sharing in matters of counter-terrorism and law enforcement respectively.

2.3.1 The Cold War as setting for contemporary intelligence

> "Certainly nothing is more rational and logical than the idea that national security policies be based upon the fullest and most accurate information available; but the Cold War spawned an intelligence Frankenstein monster that now needs to be dissected, remodelled, renationalized and made fully accountable to responsible representatives of the people."
>
> Harry Howe Ransom, 1994[174]

The 1996 US Commission, *Preparing for the 21st Century*, concluded that the focus provided by the superpower struggle of the Cold War had disappeared.[175] In a masterful command of understatement, Best, in a Congressional Library Report of 2006, suggests that:

> "During the Cold War … Intelligence agency officials working under cover as diplomats could approach potential contacts at receptions or in the context of routine embassy business. Today, however, the need is to seek information from clandestine terrorist groups or narcotics traffickers who do not appear at embassy social gatherings."[176]

The Cold War was essentially an intelligence war; its ultimate conclusion precipitated by socio-economic pressures.[177] Cold War intelligence had two aims: to find out as much about the other side as possible - political, scientific, economic and military - and to avoid conflict by matching and containing the capability of the opposition. For the intelligence community this effort was pre-conditioned by the manifestation of the threat as a military one in true Clausewitzian style - the conduct of war by nation-states or blocks of states. As a risk management exercise, the intelligence community was predominantly concerned with the capability of the threat rather than the intention; the impact of the risk rather than the likelihood. Thus it was essentially a 'bean-counting' and measuring endeavour rather than an insight and understanding one.[178] This puzzle-solving rather than mystery-understanding effort was principally conducted by clandestine means because it could not easily be conducted through open sources against targets whose commitment to concealment was routine and considerable.[179]

This is not to underestimate the contribution of Cold War open source exploitation. Both the then BBC Monitoring Service and the Foreign Broadcast Information Service adjusted their focus to provide significant contribution to the Cold War intelligence picture. Two further organisations - the UK's Soviet Studies Research Centre at Sandhurst and the Soviet Army Studies Office (SASO), the US equivalent at Fort Leavenworth - generated OSINT on capability and intention from the Soviet press, other written material and broadcast media from BBC(M) and FBIS respectively.[180] Interestingly, Pringle in 2003 and then Mercado in 2004, both looked at the use of OSINT during the Cold War but come to differing assessments.[181] While Mercado highlights the fall of the Berlin Wall as going unpredicted by closed intelligence analysts at the CIA, Pringle notes that Kremlinologists in both academia and government (non-intelligence assumed) were embarrassed by open sources. Maybe this represents more a failing of analysis or the difficulty in solving mysteries. The characteristics of contemporary society that has seen the rapid expansion of OSINT simply did not exist then.

The Cold War was also in many ways a cul-de-sac experience.[182] It removed us from the customary turbulent and violent flow of history.[183] Hough argues that: "The

conceptualization of International Relations, like the conduct of international relations, was frozen in time between 1945 and 1990."[184] He further suggests that, despite some effort at deepening and widening what constitutes security, little had shifted the 'Realist' paradigm from its dominant pedestal. 'Pluralist' and 'Social-Constructionist' theories of security, which attempt to reflect contemporary international relations beyond the application of military force on behalf of the national interest and toward an ontological notion of individual security for a multitude of 'risks', remain subordinate. The 1980 Brandt Report acknowledged the need for transition; but the apparent emasculation of the UN reflects the dominance of the nation state in international relations.[185] The dependant notion of 'the maintenance of the balance of power' still rules deliberations of the Security Council.

By contrast, the latter half of the 20th Century was also a period in which scientific and technological advances were impressive and numerous; the intelligence community benefiting enormously from them. Some of these technologies found use in the intelligence world and some were developed specifically for the intelligence world or defence more generally. Thus, a technical emphasis on information gathering grew apace: remote sensing imagery by satellite and aeroplane; beyond-visible imagery of infrared and thermal; and electronic eavesdropping in the air, down telephone wires and under-water are just some examples.[186] By the end of the Cold War this emphasis had become something approaching reliance.[187]

The fall of the wall came to represent the concluding episode in the struggle between two European-based but globally arresting ideologies.[188] Yet, the post Cold War period also released a clash within cultures and civilisations (rather than Huntingdon's prophesied clash of civilisations), and ushered in the current triumphant dominance of US-led free-market economics for all; but increasingly rejected by many.[189]

Post Cold War contemporary society has also seen the resumption of a long-time suspended clash of value-sets, exercised less now in the name of religion and more in the name of fanatical extremism on both sides; neo-liberalism and radical Islam.[190] This latest clash manifests itself in 'global', 'new' or 'asymmetric' terrorism on the part

of one protagonist[191] and consumerism disguised as freedom, democracy and choice on the part of the other.[192] Some argue that the neo-liberal value-set, particularly as exercised by the US and the UK, is responsible for both manifestations.[193]

The end of the Cold War also witnessed the demise of traditionally and habitually placed trust. The increase in innovation and independence combined with the removal of a Straussian 'common enemy' meant that we no longer fought against something.[194] Rather, we began to examine ourselves for quality of life and meaning. So far we have failed to materialise this search into any understanding of what we are for.[195] It should be no surprise then that, in a world being transformed by science and technology and in the absence of a unifying purpose, we attract a heightened sensitivity to risk. The pursuit of a global war on terrorism has failed to convince a post-Cold War, un-trusting, rightly sceptical, global public that we have found a meaningful and unifying new 'fear'. Rather, a much broader and growing awareness of environmental challenges might be returning us to a Hobbesian world, where: "(L)ife is continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short".[196]

The 'stand-off' nature of the Cold War bi-polar pseudo-conflict was replicated in the stand-off nature of its intelligence effort. Less and less intelligence activity was conducted of a 'personal' or human nature.[197] More and more resource was put into technological means. Very little was evaluated for effectiveness.[198] It is not the purpose of this thesis to discuss the rights and wrongs of the Cold War approach to intelligence gathering. However, the intelligence capability that the post Cold War world inherited and had at its disposal was effectively forged in a different era for a different engagement than one the intelligence function faces today.[199] James Woolsey, a former Director of the CIA, best summed this up when he said:

> "We have slain a large dragon, but we live now in a jungle filled with a bewildering variety of poisonous snakes, and in many ways the dragon was easier to keep track of."[200]

With regard to one aspect of the intelligence process - analysis - Clift notes that in the Cold War the intelligence analyst was king because he knew everything there was to

know about the object of their attention.[201] The analysts largely controlled 'everything there was to know' themselves. There was no Internet and very little open source to generate alternative intelligence contributions. Today information is not withheld but freely and generously given. The intelligence analyst is no longer king.[202] Today the analyst needs to 'know who knows' as much as, or possibly more importantly than, he knows about the subject himself.[203] This is the relatively new, and certainly post-Cold War, domain of open source.

2.3.2 The present day and the politicisation of intelligence

Post 9/11, it became clear to a significant majority of intelligence practitioners that the Cold War mantra of 'need to know' had to be replaced by the insistence 'need to share'.[204] Yet, intelligence practitioners and intelligence agencies are not necessarily one and the same. In the US it was four years before the subject was truly addressed by the creation of the office of DNI in February 2005, following four Presidential Executive Orders of August 2004 and the December 2004 Intelligence Reform and Terrorism Prevention Act.[205] In the UK, the creation of JTAC in June 2003, and SOCA in April 2006, went some way towards so-called 'joining the dots' of intelligence for security, law enforcement and defence bodies engaged in counter-terrorism and countering serious organised crime.

The plethora of inquiries into western intelligence matters surrounding WMD in Iraq was also catalyst for change. In the UK, the September 2003 Hutton enquiry and the subsequent 2004 Butler inquiry represented a low point in the standing and *raison d'être* of the UK national security intelligence function. In the US a similar low point emerged with the '9/11 Commission' Report and the Silberman-Rob Commission into WMD.[206] These low points both reflect and obscure the greater debate from which the inquiries emanated. That is, with respect to weapons of mass destruction (WMD) and links to Al Qaida, was intelligence pushed or pulled in order to derive a *casus belli* in Iraq? More broadly put: is intelligence used to inform policy-making or is intelligence formed to support its 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 at the time seemed to coalesce around the view that while intelligence was being selected and harvested to prop up pre-determined policy, the intelligence community was seduced into the process and failed to stop the slide.[207] Wherever the scales eventually come to rest, intelligence, both product and process, has become tainted as a result. Interestingly, Halevy[208] has suggested that, certainly as far as Israel is concerned, it is the 'intelligencisation' of politics that was the norm in his 40 years of experience rather than the reverse.[209] Kissinger supports the pre-eminent view that intelligence has always been treated as support to pre-determined policy and this properly reflects the precedence of the two disciplines.[210]

Treverton also favours the closer integration of policy and intelligence. He argues that, when Senator Patrick D. Moynihan called for the abolition of the CIA because it could not predict the collapse of the Soviet Union, he was half right.[211] Treverton suggests that, rather than disbanding the CIA; it should be broken-up and dispersed to all the departments of state precisely in order to get alongside the policy-makers. This would address the modern challenge of informing policy about what they should be looking out for and responding to its requests more speedily and cogently. Again this is a peculiarly US response. Treverton further notes that the UK's JIC system does much to bridge the gap between policy and intelligence although presciently warned in 2003 that such a relationship was fraught with dangers of politicisation.[212]

Betts summarises the politicisation debate according to which former senior US intelligence official you concur with.[213] The Kent model of politicisation is one of avoidance; characterised by objectivity of analysis and distance from policy-makers. The Gates model is one of engagement; characterised by closeness and utility of analysis, attempting contextualisation rather than politicisation. Shulsky and Schmitt create a degree of resolution to the debate by reminding us that objectivity, as Heizenberg discovered, is not a mortal or even natural virtue.[214] They suggest that the intelligence function is inescapably shaped by policy. Thus, we err to engagement - like it or not. However, rather than fret about politicisation we should concern

ourselves with 'independence'. The independence of intelligence, they conclude, is ultimately guarded by: "(T)he backbones of the chiefs of the intelligence services and their willingness and ability to protect analysts from outside pressure."[215]

However, intelligence's own 'failings' are not the only drivers of intelligence reform. Still greater forces are at work; reflections of contemporary society that are even more capable of overwhelming the intelligence function than Hutton, Butler or the 9/11 Commission. The intelligence capability needed today, (perhaps its lifeline), can be found in the practice of open source information gathering. The formal treatment of OSINT is a consequence of contemporary contextual influences that are bringing about its potentially starring role as key element of intelligence reform.

2.3.3 Intelligence reform: What practitioners say

Cries for intelligence reform always follow a fall.[216] In most cases reforms of some kind, structural, functional or organisational, do occur. 9/11 and Iraqi WMD follow the normal pattern. What has not occurred is reform in anticipation and prevention of a fall in the long quiet periods between orgies of intelligence chaos.

The literature on intelligence reform is growing. Respected former-intelligence professionals have contributed to the debate: Treverton, Odom, Markowitz, Steele, Berkowitz and Goodman, Hulnick, Johnson, Lowenthal, and Holden-Rhodes to mention a few.[217] Additional contributors appeared in an entire issue of *Intelligence and National Security* journal devoted to the debate under the title: 'Twenty-First Century Intelligence'.[218] Several points stand out:

- The contributors all have extensive clandestine intelligence experience.
- They are mostly American (those cited above certainly are).
- They all recognise the compartmentalised culture of the intelligence community that favours secrecy over dissemination of information.

- They all have concerns about duplication, measures of effectiveness, intra-community competition rather than cooperation, value for money, politicisation and risks beyond merely security.
- They all recognise the potential of open source intelligence.

The reviews into the conduct of intelligence by various oversight committees and intelligence commissions, since 1947, support the points above. In short, they argue that intelligence, as presently constructed, is not best fit for the 21st century.[219]

This most recent literature also addresses fundamental value-sets as much as organisational or functional change. Most of them to varying degree acknowledge contemporary global societal changes that are impacting upon their governments and thus their intelligence function. However, the acute observers of globalisation, risk and changing societal expectations - the context for government let alone intelligence - still reside outside the intelligence community. As the author has argued elsewhere - increasingly everything is connected to everything else.[220] This may be so; but more importantly, when the froth of Iraq dies down and 'new' terrorism is placed in perspective, these interconnections are slowly coalescing in people's minds into the real challenges that face humanity, which are perceived inadequately addressed.[221]

Recognising that forces of change are coalescing with perceived intelligence failure, intelligence practitioners engaged in the reform debate have made some reasonably uniform comments:

- Intelligence is about being in the information business not the secrecy business.[222]
- Compartmentalisation, security and turf-war lead to a culture of secrecy that prohibits information sharing.[223]
- A preoccupation with 'current' intelligence reporting to fill gaps in knowledge precludes the cultivation of deeper analytical insight that might lead the way to alternative points of view.[224]
- Confirmatory evidence is rewarded while discomfimatory evidence is discouraged or discounted.[225]

- The need for secrecy is juxtaposed to the need for debate and discussion.[226]
- The intelligence community, as it is presently constructed on national intelligence machineries rather than being cognisant of a global commons,[227] does not have the preserve on knowledge.[228]
- Risk theory should be understood and incorporated into intelligence methodology ranking alongside analysis so that the intelligence function can be directed and resourced appropriately and so that the intelligence community knows what its priorities are.[229]
- The tendency to spend resource and budget on high technology intelligence solutions at the expense of Humint and latterly OSINT is misguided.[230]
- Intelligence should treat risk on a global rather than nation-state level. Global risks already constitute humanity's greatest challenges, while nation-states, particularly the US and UK, act on behalf of consumer oriented elites to the neglect and ignorance of their own populations let alone the rest of the world.[231]

The intelligence community ethos has generally and genuinely been to get to the truth. To manage contemporary risks requires the best available information and not just a selection based upon closed sources. If this is left to TCSOs as moral authority of last resort then the other parties in the global commons, notably MNCs and nation-state governments will have an open field to do whatever they want in the name of the people, but not necessarily in their best interest.

A nation-state's security function, of which intelligence is a part, can be seen more usefully in contemporary society as its risk management apparatus; from risk identification and awareness through assessment to treatment and control. Intelligence's role is more akin to that of a research and development function; sufficiently remote from the short-term desire for efficiency, and oriented to the long-term responsiveness of innovation.[232] In political terms: not in the service of the government, but serving the long-term interests of the nation.

2.4 Open source intelligence (OSINT)

> The sharing of information, cooperation in the gathering of intelligence, and mutual planning to reduce strategic vulnerabilities, would seem the way forward. So far, however, little of this has been forthcoming.
>
> Anthony Giddens, 2002[233]

The literature of academic quality, objective in nature, and related specifically to open source intelligence (OSINT) is extremely limited and rarely concentrating on OSINT as a discrete subject. More frequently it is incorporated, as a sub-set of the so-called 'intelligence reform' debate. By contrast, the practitioner literature is extensive. However, it has emanated almost exclusively from one source swamping most other comment, and seems polemical and rhetorical in nature.

The 'intelligence reform' literature acknowledges open source as a phenomenon reflecting the contemporary transformation in ICT, but does not discuss its treatment beyond the 'network-centric' model. The networked nature of contemporary society is more a comment upon ICT than the intrinsic worth of open sources. This same literature records anecdotally that OSINT is underutilised at best and mistrusted at worst. However, evidence of direct criticism of OSINT is not obvious. Two papers specifically discuss the validity and shortcomings of OSINT: Pringle argues that open source information can be ambiguous and therefore not so useful as closed;[234] Hulnick refers to the challenge of 'blowback', where false information (misinformation or disinformation) is taken for truth and found more convincing than intelligence analysis. The criticism is cautionary rather than disparaging and, as Johnson infers, is as much a feature of all intelligence as OSINT specifically.[235] Hulnick also suggests that blowback results from the exploitation of media sources; [236] but one might equally argue that clandestine methods have a similar challenge. The extraordinary reliance upon Ahmed Chalibi by the US Government in preparation for the Iraq War 2003 represents a significant case of blowback.[237] However, an understanding of how the media come to represent point sources for the amplification of risk messages is important, and perhaps more useful than setting them up as 'whipping boy'.[238]

It is worth re-emphasising that there is nothing intrinsically new in open sources of information. To take a reasonably distant example, *The Times* regularly printed a column called 'Foreign Intelligence' during the Napoleonic Wars.[239] Similarly, the exploitation of open sources by intelligence agencies is not new.[240] In the 1920s, Vernon Kell the founder of what became MI5 was already using private intelligence companies to counter the Bolshevik threat, including Conservative Central Office to unveil what was to become a *cause célèbre* – the Zinoviev letter.[241] Prior to 1914 and after the outbreak of WW I, Mansfield Cumming's MI6 was running a German network of British officers engaged in monitoring German naval developments around key Baltic ports. Despite censorship and with trained analysis these officers were able to obtain a great deal of information from the newspapers; openly, legally collected and extremely valuable.[242] The American experience is similar.[243]

What is new is the sheer magnitude of open source information as a result of the ICT transformation. But which transformation (?): the invention of the alphabet in Ancient Egypt around 3000BC; the invention of movable type and the printing press by Johannes Gutenberg *circa* 1450; the establishment of the first radio broadcast station by Guglielmo Marconi in 1897; or the creation of the world wide web by Tim Berners-Lee between 1989-1990. As Reuser points out, the volume of data held digitally is still exceeded by the analogue variety held in magnetic and film formats.[244]

2.4.1 Definitions

While the definition of intelligence remains contested, there is of course a wider interest in, and study of, the role of information in decision-making beyond the intelligence community. Indeed, decision-making absent of information in most aspects of life might be considered foolish; although, Taleb argues convincingly that when it comes to 'forecasting' most decisions are taken precisely in the absence of information.[245]

All information is collected, collated, organised data. It is the prerequisite for creating, in combination with analysis, knowledge.[246] Knowledge is confusingly interchanged with intelligence but the distinction is weak and rapidly becoming a semantical debate

rather than one of substance. Yet, intelligence is treated as a specialised form of knowledge.[247] It is simply a more appropriate and accepted term in government and public sector circles (by dint of tradition and history more than anything else). Knowledge is an equivalent, more modern term, increasingly in use in private and non-public sectors. In fact it is much more helpful to think of knowledge as a product and intelligence as the process whose product is knowledge.[248] For the sake of completeness but not discussed further: wisdom has been described as knowledge or intelligence combined with experience and the passage of time; and insight as wisdom combined with understanding.[249]

Intelligence, as support to decision-making, has three key and distinguishing features. First, people - analysts to be precise - who create knowledge.[250] Second, data, which is collated into information and upon which analysts can work. Third, a 'target' or requirement against which such work is directed. Where these three intersect constitutes the 'business' of intelligence. Yet, such knowledge that merely informs the analyst, who creates it but cannot share or disseminate it, remains at best a secret and at worst self-indulgence at the taxpayer's expense. Thus, implicit in intelligence's support to decision-making and action is its communication and dissemination. In this description of knowledge creation, it is unimportant whether the data or the process of converting the data into intelligence is 'secret' or not. Here, a useful connection can be established between knowledge in its closed variant - intelligence - and open source exploitation. Open source exploitation, at the very least, presents otherwise unseen data into the decision-making process, which intelligence supports.

Lowenthal has defined OSINT as the analytical exploitation of information that is legally available and in the public domain.[251] That is to say the information is neither acquired clandestinely through espionage or illegal means, nor is it "closed" to the public by government or commercial sensitivity. Of course the resultant analysis of open sources may very well be designated sensitive and the means of collection may be anonymised. Lowenthal expands the definition slightly to incorporate a distinction between OSINT collected by the public sector intelligence community, and OSINT collected by other members of the intelligence commons.[252] He argues that by virtue of

the opportunity for OSINT to be verified and corroborated against closed intelligence it must be of a different nature. Logically, and as this research shows, the reverse must also be true; that closed can be verified against open. In this regard, Treverton argues that a real value for closed intelligence can only be measured by comparison to what is available openly.[253] Thus, he reinforces the argument for OSINT to become part of the community intelligence effort.[254]

The US DoD constricts the definition of OSINT to: "Information of potential intelligence value that is available to the general public".[255] This definition omits legality and thus at the very least suspends the rules of copyright. It also omits any mention of analysis, critical to the production of intelligence. The cursory treatment of OSINT by the US DoD at the time of this document illustrates their view if not understanding of the phenomenon.[256]

Treverton describes open source as everything else besides the intelligence's specialised 'ints'.[257] He goes on to suggest that: "More information could be had by looking, not spying"; and: "(But) the most important information resides not in the world of secrets but in the world at large".[258] While the sentiment behind this definition is understood, the fact remains that sometimes entities do not openly disclose information for others to find. Closed and open are not mutually exclusive and not in competition.

It is worth noting a passing recognition of 'open source', albeit back-handedly, by the UK Intelligence and Security Committee: "Their (Intelligence Agencies) task is to inform decision-makers and allow the formulation of policy to be based on more information than is available from open sources".[259] It is difficult to gauge whether this is a withering put down of open source or confirmation of their position as firmly in the clandestine camp. Either way it demonstrates an ambiguity to engagement in the entire information business. Equally, in 2005, the UK's then Intelligence and Security Coordinator displayed mixed views on the efficacy of open source - acknowledging its potential while cautious about its validity.[260]

Commensurate with many changing aspects of contemporary society, OSINT is clearly both a product of the ICT transformation and a tool to deal with it. Notwithstanding the contestable and problematic issues of what is legal and what is public, this thesis uses the following definition of open source intelligence:

> "The exploitation of information legally available in the public domain."

2.4.2 OSINT sources

The Internet, and before that newspaper 'cut-and-paste', remain the stereotypes of OSINT. This severely underestimates the field. Indeed, the Internet is not of itself a source, merely the means by which sources are accessed, stored and supported.[261] Of course, the power and potential of the Internet to facilitate open source access increases daily (approximately one million 'pages' are added each day). For example a recently stated aim of Google Print is to make the full text of all the world's books searchable by anyone online.[262] It seems inevitable with increased digitisation that it will in time become the first port of call for open source collection. However, a 2001 CIA study into the future of the Internet as a continuing shaper of contemporary society, and intelligence implicitly, considers three alternative scenarios to the rosy one here, in which two of those scenarios depict a shrinking digital environment.[263] Combine this with the estimate that in 2002 the Internet facilitated access to only 10-20 percent of all OSINT then the implications of the requirements for sophisticated, trained and properly resourced open source analysis are stark.[264] The US DoD recognises the Internet as a communication means for itself (SIPRNET and NPRNET) but have hitherto (2005) largely left its exploitation to what was once FBIS.[265] They are not alone. Contemporary Jihadist movements regard the Internet as the main way to communicate with the outside world. They know it, and the world's media monitor their sites waiting for announcements.[266]

The categories of open source are blurring, but they might usefully be categorised broadly as follows:

- **Media**
  - Traditional media broadcast such as radio, television and satellite.
  - Traditional print media such as newspapers and magazines.
  - Variations of the above two in digital format and for the most part accessible via the Internet - digital media.
  - Aggregated compilations of the above accessible on-line and referred to as 'commercial on-line premium' or 'online content' such as Factiva, Lexis-Nexis or Dialog for global print media coverage, and BBC Monitoring for all forms of traditional as well as new forms of media.

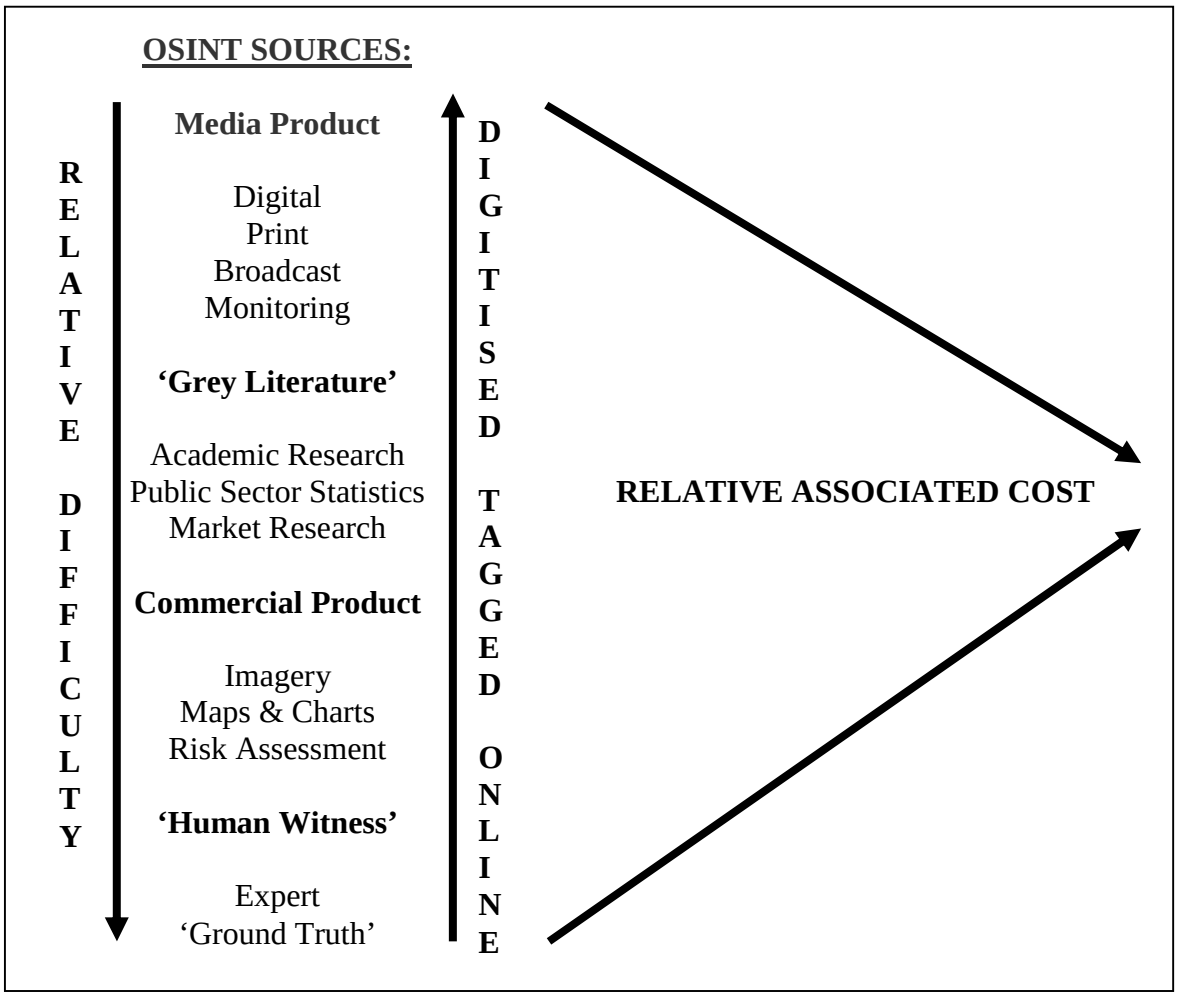
- **'Grey Literature'**
  - Academic research, access to academic journals and specialists.
  - Conferences, exhibitions, trade shows, expositions, conventions and meetings.[267]
  - Public sector statistics and databases.
  - Private sector market research and databases.

- **Commercial Product**
  - Specialist technical/tactical coverage such as Janes, Oxford Analytica, the Economist Intelligence Unit and other private information brokers (PIBs).
  - Commercial imagery – there are at least eleven private (commercial) high-resolution (near 1m) remote sensing satellites available to credit card holders.[268]
  - Mapping specialists such as Eastview Cartographic, suppliers to the US DoD for Afghanistan, Iraq and most recently Iran.[269]
  - Risk assessment.
  - Private sector market research and databases.

- **'Human Witness'**
  - Overt human observers or 'ground truth' expertise – the most valuable means of ascertaining 'ground truth' such as International Alert, the Red Cross, Amnesty International, businessmen, journalists, travellers, academics and refugees.

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 2001 estimate that 29 languages are considered minimum entry for a complete intelligence picture.[270] (In 2004, Steele referred to 33+ languages as minimum entry).[271] Furthermore, being in the public domain does not necessarily imply that it is also transparent, freely available, accurate, complete or even truly 'public'. It will be formed by value and bias, it may be in a foreign language, it may be exchangeable for money or disclosure of personal information, it may be second, third or fourth hand and it may be difficult to find or difficult to get hold of. In all these limitations and many more besides, it carries integrity issues no different to closed information. Equally, just because OSINT is collected from open source does not mean that it will remain open. OSINT often becomes classified to preserve anonymity of the collector, to protect the method of collection and to protect operations or intent as a result of aggregation. Again, this is entirely similar to closed information. More contentiously it is classified simply by virtue of who is collecting it. Figure 2.4 below outlines the OSINT categories and their associated degrees of difficulty to obtain, cost and digitise. The arrows indicate increasing direction.

Figure 2.4: OSINT sources



Source: Author

However, it has also become apparent during the course of this research, and coincidental with the post 9/11 years that several variations on a theme are emerging. It is no longer sufficient to simply suggest that everything outside the traditional closed intelligence environment is, by implication, open. At least two other avenues of activity are emerging, which blur both the traditional understanding of intelligence as well as the distinction between open and closed information. First, there has been a tremendous shift in all aspects of security away from it being provided by the state towards it being supplemented, if not replaced in some areas, by the private sector. Second, there has been a growing effort by information specialists and the ICT community generally to engage in security matters through the digital economy. The former has in some sense created a parallel, albeit emergent, intelligence industry to that

of the government. The latter has created an additional source of information for use by public and private sector intelligence practitioners. For example, airline bookings, mobile phone records, drug prescriptions, property records, loyalty cards, and many more, now form part of a digital cornucopia of databases held by a wide variety of organisations.[272] Some of this 'private' information is perhaps beyond the traditional definition of open source information - legally available in the public domain - but is certainly exploited by the intelligence arms of law enforcement. Not insignificantly it also raises questions of civil liberties and 'own-citizen' surveillance.[273]

It is not clear how these avenues will proceed; separately and randomly like 'bumper cars', or become something more cohesive. However, it is pertinent to note that the subject of intelligence is accelerating away from the Cold War understanding of a closed government operation. Similarly, it seems unlikely that the exploitation of open sources of information will be able to occupy a discrete 'space' unmoved by the buffeting of a changing technological environment, let alone a social one.

2.4.3 OSINT as intelligence

Intelligence or knowledge, regardless of the origin of its precursor-information (open or clandestine), must be timely, accurate, relevant and verifiable. 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. Indeed, as the results chapter shows, these sources, once verified, become key inputs for OSINT exploitation. 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 at worst psychotic. Classified 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:[274]

- 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?
- Coverage - is it relevant i.e. adds to understanding or is it just interesting or circular reporting?

Common to all organisations practicing OSINT are the following three aspects:[275]

- They pay for and control data and data-experts that create information.
- The information they put into the public domain, for a variety of reasons, represents only a small proportion of what they know.
- Between groups, organisations and individuals there are barriers to the flow of information.

These aspects constrain the best possible decision-making because they constrain the best possible use of information. They create inefficiency because the sources are often duplicated and therefore "paid for" several times over. Although this is commonly recognised as a knowledge management challenge for all organisations it is particularly pertinent to intelligence

2.4.4 OSINT anomalies

OSINT need not necessarily be obtained openly in that the acquirer leaves a calling card. It can be discretely acquired. Given that one of the qualifying definitions of intelligence is the covert acquisition of information that the owner does not wish released, OSINT acquired discretely only fulfils the latter of the two criteria that form its definition - legally available in the public domain. However, it does fulfil the security requirement for protecting methods and intent. That the sales of 'Annonymizer' to the US public sector have rocketed over the last few years indicates that covert open source exploitation is being undertaken.[276]

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, the need for secrecy must be legitimate.[277] Classification without justification, preventing communication and dissemination rather negates a principal attribute of open source, namely its ability to be shared. Regrettably, 'need to know' has become a debate complicated more by issues of organisational culture and personal vested interest than operational security. The mounting dilemmas of global, contemporary, 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. The 2004 '9/11 Commission' articulated the desire to replace the 'need to know' mantra with the 'need to share' imperative.[278] This was subsequently enacted in the US, although only with regard to terrorism, through the creation of an Information Sharing Environment (ISE).[279]

There is a further anomaly thrown up for the open source world that is as much due to a reaction to the traditional intelligence model and modern governance as it is a product of the information explosion. Information that is 'leaked' or placed in the public domain illegally becomes available to exploiters of open source information. In this respect misinformation and disinformation rules apply as much to open source information as it does to closed. It also becomes ethically or perhaps legally debateable

as to whether such information should be harvested. Such disclosures perfectly illustrate the role of OSINT as both open source and 'openness'. Taken with all the other more normal open sources of information it is becoming increasingly difficult for governments and organisations to keep any secrets at all. John Perry Barlow best sums this up:[280]

> "The secrecy paradigm has lost, the openness paradigm has won! It is my position that trying to embargo knowledge is a little bit like trying to embargo wind. This stuff is incredibly leaky, it's very volatile, it's almost a living form in a sense that it is self-propagating. I think you have to accept the idea that we are moving into an environment where information – if it is interesting to people – is going to get out. And there is nothing you can do about it. This is not necessarily a bad thing!"

With regard to disinformation and information assurance generally, Hulnick argues that there is a downside to open source exploitation. Knowing that open sources are exploited means that 'adversaries' can inject disinformation to confuse or mislead analysts - 'blowback'.[281] This seems a perfectly credible assertion; but it is as equally applicable to closed sources or secret intelligence as it is to open. As has been suggested, a reliance on émigré reports prior to the Gulf War 2003 contributed to the embarrassment of intelligence communities globally.[282] Steele and other advocates of open source would argue that the sheer plethora of open source militates against the 'single-source' effect. However, Hulnick's more pertinent point, that putting across an analysts' considered view against an instantaneous and often knee-jerk media view of a situation, is being addressed in the risk management discipline under the Social Amplification of Risk Framework as well as in political and journalistic spheres.[283]

2.4.5 OSINT as private intelligence industry

There is a growing awareness of the term OSINT and the utility of OSINT product, certainly within the private security sector, and more widely to customers of the private security industry. As a result the OSINT industry is growing and establishing itself as a quasi-privatised intelligence sector. The worlds of competitive intelligence for economic and commercial intelligence[284] and knowledge management in public and private sectors demonstrate and utilise open source information gathering.[285]

The explosion of information and its distribution to a variety of centres of information-handling excellence is exemplified by the recent establishment of a number of commercial information-brokering companies pertinent to the security sector and similar such departments within private security companies and larger global corporations.[286] This creation of a corporate sector capability, either superior to public sector, where it competes, or in filling gaps where the public sector no longer operates, seems inevitable given pre-9/11 reductions in the national intelligence machineries. The corporate sector together with academia and the media is steadily creating a formidable private risk and security management sector (not solely limited to OSINT) that is usefully contributing to a national and international security network.[287] This consumption, production and distribution of information within the corporate sector contribute to both the informing of the public at large and filling the communication gap in security risk matters. The contribution of private information brokers is examined in detail in Chapter Four (4.2).

2.4.6 OSINT and public sector information gathering

Like every organisation, those organisations within the public sector suffer the overriding dilemma of the distributed information explosion - too much of it. Nye refers to this 'paradox of plenty' as enhancing the credibility and trust dilemma for policy-makers. On the one hand, too much information leads to a scarcity of attention by recipients. On the other, this inattention is complicated by the heightened scepticism of a sensitised public. Under the new information age conditions, open sources increasingly contribute to the efficacy of 'soft power' as exercised through 'public diplomacy'.[288]

Additionally, the public sector must also bear the additional straightjacket imposed by the classification of information into restricted information or 'intelligence'. The culture of secrecy engendered by classification paranoia (as distinct from the incisive application of secret intelligence) has a detrimental affect on the process of information gathering that might lead to action or 'knowledge'. It becomes the process rather than the product that dominates, which is ultimately detrimental to decision-making. This

might be fine for the internal consumers within organisations of the public sector (although given the dependency upon barriers within hierarchical organisations this seems unlikely) who perhaps feel that they do not have to share their information outside their own boundaries, but it underestimates the use that that information could be put to by equivalent or superior expertise outside the public sector.

The culture of secrecy also fails to appreciate how useful this information might be in communicating security risks at the outset of any new emergent threat in order to engender trust. This trust is necessary to support decision-making, security risk management and action so that it will be accepted and acceptable. An inability or unwillingness to communicate risk will only engender distrust and unacceptability. Similar criticism can be levelled at the private sector with their own brand of restricted information - commercial in confidence.[289]

The justification for information restriction seems as much dependant upon being handled by a 'classifying' organisation, as it is genuinely contingent upon the content and the nature of the information itself. In response to the disclosure of OSINT's 80 percent contribution to final intelligence product, Steele coined the phrase - "no classification without justification" as a way of reversing the knee-jerk tendency to classify.[290]

Fixation with the classification of information leads to inevitable information constriction rather than dissemination. Thus it diminishes informative value. Secrecy for secrecy's sake, whether as a pathological response to protect future positions or as a result of simple bureaucratic abuse, will negate the positive impacts of influencing risk perception, enhancing risk identification and improving resilience and competitive advantage in the security sector. This is not to suggest that classification does not have its place. Rather it is to say that OSINT should be more fully exploited to allow greater devotion of time and resource to the closed gathering of sensitive, vulnerable, tactical intelligence. Private sector and academic information-brokers seem well placed to take on much of that work. Johnston sums up the classification debate:[291]

> "Another organizational norm that contributes to the confirmation bias in the Intelligence Community is the selection and weighing of data according to classification. Secrets carry the imprimatur of the organization and, in turn, have more face validity than information collected through open sources.[292] … Because it is generated and packaged in specific formats using specific processes, classified information lacks the diversity that is inherent in open information, and this contributes to confirmation bias."

Four additional comments are worthy of note. First, is it right that the taxpayer should pay for something that is derived from open source but subsequently not made available to the public? Second, if the capability exists in the private sector is it efficient for the public sector to duplicate the process? Third, as information increases in volume and becomes more and more distributed to individual centres of excellence, a hierarchical, centralised system of handling it will only struggle to cope, becoming increasingly less responsive to and less representative of the society for which it acts. Fourth, there is considerable evidence to suggest that public sector information gathering agencies duplicate and compete rather than share amongst themselves. Much has been written about Northern Ireland in the 1970s and 1980s illustrating the competition for "scoops" between RUC Special Branch, MI5, MI6 and Army Intelligence, the ramifications of which are still being felt today.[293] The same is true of the private sector with the qualifications that, consumers of information do so precisely in order to compete, and the providers of information are whittled and channelled in time by market forces and competition to reduce duplication.

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. The inference is that if OSINT is such a significant and growing input to private sector decision-making then public sector intelligence-based activity should sit up and take note. The public sector has noted the inference. The issue for OSINT is no longer its validity or usefulness rather how could it be developed, institutionalised and rolled out as a discipline common to government intelligence analysts and commercial knowledge workers alike.

2.4.7 OSINT's influence

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 security, law enforcement, and defence or any other function of society. But in an age characterised 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 policy-making weakness. Information gaps create communication credibility challenges, which lead to mistrust and a destructive cycle of stigma, increased mistrust and further credibility challenge for all policy-makers.[294]

Why is OSINT so good? This presupposes that it is good relative to something else and that 'something else' is traditionally held to be closed intelligence obtained through espionage. The more perceptive organisations that require knowledge to function are beginning to appreciate that the two are not in competition but mutually supportive.

At the level of intelligence *qua* process and product, and as an 'intelligence discipline' in its own right alongside the clandestine disciplines (Humint, Sigint, Elint for example), the main benefits of OSINT include the following; it is fast, flexible, dynamic and cheap;[295] it is communicable, sharable, trust creating and partner–forming, particularly for multi-national organisations such as NATO and the UN engaged in peacekeeping operations, where nationally supplied intelligence has a restricted flow and therefore limited value;[296] 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;[297] it contextualises the intelligence requirement both historically and currently, providing the matrix in which the clandestine intelligence disciplines 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 disciplines for their own more concentrated espionage; it provides 'cover' and risk

communication possibilities for the other disciplines; and it provides 'horizon-scanning' to focus the other disciplines. However, with the exception of the last statement (all the intelligence disciplines can do that), it is irresistible to compare open source with clandestine in each of the above categories. Enlightened organisations have undertaken this comparison and been persuaded by the relative benefits! The US Navy Commander of the lead wing into Baghdad in 1991 sums up the benefits better than most:[298]

> "If it is 85 percent 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."

OSINT can usefully contribute to the wider management of risk by enhancing the informing of perception, where little or none exists, through utilising risk communication theory and generating virtuous circles of trust and confidence rather than mistrust and stigma. 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.[299] Such risk communication has to be conducted in the knowledge that all risk communication is a reflexive phenomenon. That is to say, where the parties to communication ('transmitters' and 'receivers') are conscious agents, each is influenced by the decisions and messages of others.[300]

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 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.[301] 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.[302] 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.

2.4.8 The '80 percent plus' rule

> "Because of its glamour and mystery, overemphasis is generally placed on what is called secret intelligence, namely the intelligence that is obtained by secret means and by secret agents … In time of peace the bulk of intelligence can be obtained through overt channels, through our diplomatic and consular missions, and our military, naval and air attachés in the normal and proper course of their work. It can also be obtained through the world press, the radio, and through the many thousands of Americans, business and professional men and American residents of foreign countries, who are naturally and normally brought in touch with what is going on in those countries."
>
> Allen Dulles, 1947

The quote above formed part of the testimony by Allen Dulles, Director CIA, to the Senate Committee on Armed Services 25 April 1947.[303] His testimony was only nine pages long and hastily written; but in it, as Markowitz has noted,[304] he began the process of the demystification of the art of intelligence. Dulles added in that same testimony:

> "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."

These observations by Dulles represent the first recognition of the value of open source information together with a quantitative estimation of its contribution to the US intelligence function. Anecdotally, today, this figure may be nearer 90 percent and, for some all-source intelligence agencies, is the preferred 'knowledge' of choice.[305]

The perceived efficacy of OSINT by many other eminent practitioners and more importantly satisfied customers is increasing.[306] Elcock, Oehler and Scalingi consider that OSINT provides 80 percent of final product for arms control and arms proliferation issues.[307] Hulnick, in examining the Cold War, suggests that 80 percent of the data

suitable for analysis on the Communist enemy could have been taken from open sources.[308] EUROPOL has indicated to the author that the contribution might be as high as 95 percent for counter-terrorism issues.[309] Scheuer, the former head of the CIA's special Bin Laden unit has said that: "90 percent of what you need to know comes from open source intelligence."[310] Steele's Open Source Solutions' view is that, on balance across the board, OSINT can and should provide 80 percent of what any government needs to know and 90 percent for private sector organisations.[311] The 1996 Aspin-Brown Commission remarked that: "In some areas … it is estimated that as much as 95 percent of the information utilized now comes from open sources."[312] Finally, but not exhaustively, in December 2005 at a meeting of the Oxford Intelligence Group, Nolte stated that 95-98 percent of all information handled by the US intelligence community derives from open source.[313]

Responding to the report of the 1997 US Commission on Secrecy in a letter to Commission Chairman Senator Daniel P Moynihan[314], the grand master of US foreign policy George F Kennan, wrote:

> "It is my conviction, based on some 70 years of experience, first as a Government official and then in the past 45 years as a historian, that the need by our government for secret intelligence about affairs elsewhere in the world has been vastly overrated. I would say that something upward of 95 percent of what we need to know could be very well obtained by the careful and competent study of perfectly legitimate sources of information open and available to us in the rich library and archival holdings of this country. Much of the remainder, if it could not be found here (and there is very little of it that could not), could easily be nonsecretively elicited from similar sources abroad."[315]

By the mid 1990s the US government's (CIA) Community Open Source Programme had officially estimated the open source contribution to be in the range of 40 percent over-all, with the actual contributions, depending upon target difficulty, ranging from ten percent in very denied-area, secret-issue matters, to 90 percent on international economics.[316] This and Dulles' work are the only two genuine data-points for the evaluation of OSINT's contribution in the US by methodological process and by such authoritative parts of the intelligence community. There has been no similar effort anywhere else. Indeed, beyond subjective assessment there is no quantitative research

to support these figures. Markowitz suggests that much of the chatter surrounding this claim might be no more than circular reporting of Dulles's original estimate.[317] Once stated by respected members of the intelligence community it passes into lore.[318]

Regardless of the percentage estimate of contribution or value, which, if the great and the good of the intelligence community are to be noted, appears conclusively high, the obvious questions seem to be: contribution to what, percentage of what or value of what; and how did they evaluate or calculate the figure? Is it 90 percent of a final intelligence report or 90 percent of action outcomes, that is to say an arrest or a threat interdiction. They reveal no more beyond an estimate of input to the intelligence process. It does not tell us how this input is related to output and thus how effective it is. Interestingly, the US Army, when they say that it is to do with, "…determining whether PIRs (priority intelligence requirements) have been answered" have actually put their finger on it, but do not describe how it might be achieved.[319] Indeed, the US Joint Chiefs take it further in 2004, when they recognise that intelligence evaluation is undertaken by the customer based upon: "the attributes of good intelligence: anticipatory, timely, accurate, usable, complete, relevant, objective, available".[320] Before evaluating the efficacy or otherwise of open source exploitation, it seems crucial to understand how it is effective absolutely, and how it is effective relatively in relation to closed intelligence.

The UK Intelligence and Security Committee also recognise the need to relate inputs to outputs as part of top-level management tools ensuring 'business' objectives are met within the Intelligence Agencies. To that end, and in common with other public sector organisations, this 'soft' measurement of business objectives within the Intelligence Agencies are now determined by Public Service Agreements and the Service Delivery Agreements that stem from them.[321] In common with other public sector departments the Intelligence Agencies are transferring to a resource–based accounting process. Yet, it is not clear from the literature how these agreements work or how they impact effectiveness as far as the intelligence agencies are concerned. This difficulty in deriving meaningful outcomes is not confined to public sector organisations. Wilson argues powerfully, that mankind may be 'Paleolithically' hardwired to fixate on the

short term and, 'Pavlov-like', default to the self-interested and greedy.[322] It is not an exclusively human trait; yet it is a chosen one on our part. We are probably the only species who can consciously recognise that short-termist, self-serving habits are contextually detrimental; but persist with them.[323] Whereas the 20th Century has been 'measured', at least in economic terms, by GNP (gross national product) the 21st Century is in need of something more comprehensive and meaningful such as the 'Genuine Progress Index'.[324] There seems no reason why intelligence should not aspire to humanity's greatest challenges; part of which may lie in unravelling contemporary economic rational thinking including its own.

Odom, with regard to US intelligence, also bemoans the fact that nowhere within the intelligence community are inputs related to outputs:

> "Because the DCI has never made the effort to impose a similar system (to the Defense Department) on resource management in the Intelligence Community, its consolidated Intelligence Community budget does not effectively relate inputs to outputs."[325]

A similar situation seems to exist within the UK intelligence community although not so openly discussed by such a senior intelligence community representative as Odom. In both the UK and US detailed disclosure of annual budgets remains closed information. In its annual reports, the UK Intelligence and Security Committee redacts out everything bar the total figure for the UK Single Intelligence Account (SIA).[326] The US does not willingly release that much. The pressure in the US to reveal these figures is significant. Led by the Federation of American Scientists, the argument for disclosure is fundamentally linked to imperatives of good governance.[327] There is certainly no obvious effort to relate inputs and outputs for open source exploitation in the UK intelligence community.

Thus, contribution should not be confused with effectiveness. The former might usefully be interpreted as a measure of input and the latter might usefully be interpreted as a measure of output in relation to objectives.[328] Tussing indicated the requirement for a new measure of effectiveness within the intelligence community: "instead of traditional benchmarks of quantity and quality of data gathered, the community's main

goal should center (*sic*) on how much of that data was used".[329] However, he does not suggest how that might be done or indicate that a logical evaluator of effectiveness of evaluated and interpreted data might simply be the customer.

The debate over 'effectiveness' is important in one key regard. If a measure of effectiveness is derived then it may prioritise or at least influence the treatment of OSINT within agencies and across the national intelligence machinery. But, the anecdotal 80 percent rule is simply that. Furthermore, it is difficult to verify and does not really demonstrate efficacy. Attempting to demonstrate efficacy might contribute to an understanding of how the exploitation of OSINT is impacting upon intelligence and any implications for policy.

2.4.9 Intelligence reform: Open and closed

> "And for these new challenges, many open source materials may provide the critical and perhaps only window into activities that threaten the United States."
>
> Silberman and Robb, 2005[330]

As early as 2001, the US intelligence community, under the remit of the Quadrennial Intelligence Community Review, was beginning to tackle the increasing problem of integrating open sources of information with more traditional closed sources.[331] The initiative was established to help it deal with the newer threats of terrorism, drug-trafficking and organised crime. Events of that year overtook the process and the challenge was not addressed until the DNI created the Open Source Center in 2005. Meanwhile, reformists argued that intelligence without OSINT was simply not the 'full package', and practitioners argued that the culture and security of a closed environment leading to stove-piping and compartmentalisation stifled any open source operation.[332] And, at the tops of the respective agencies and policy directorates, the need to share was becoming a common cry. This came full-circle in December 2004, when the US House Report on intelligence reform recommended the creation of an Information Sharing Environment under the direction of the newly created DNI to do precisely that with respect to counter-terrorism.[333]

That there are two parts to the information business - open and closed - is not in doubt. But the walk does not yet match the talk on sharing. Perhaps, now, during this introspective period for intelligence, post Cold War, post the host of foreign-policy shortcomings of the 1990s, post 9/11 and post Iraqi-intelligence, that intelligence reformers must consider not whether but to what extent intelligence is to be involved in both halves of the information business. If government and national intelligence machineries choose not to fully engage with the open half then the consequences may well be that:

- Intelligence communities will only be able to solve tactical, short-term puzzles by secret means, contributing little to the communication of the realities of risk and thus trust.
- Government policy and decision-makers will come to use private information brokerages of open source intelligence more and more, where the market style relationships of producer-consumer are king.
- TCSOs will only increase their influence and moral authority through the exercising of reputational risk management. Given the perceived record of nation-state governance around the world, with the exception of the Scandinavian countries, this may be no bad thing.[334]
- The politicisation of intelligence, interpreted as a loss of independence and thus integrity, may intensify when a closer but equally independent relationship between policy and intelligence should be developing. Telling power what it wants to hear may unwittingly and regrettably become the norm.

Treverton, when addressing why the intelligence community should process open source information rather than just secrets, states that: "... because assessing the value of secrets requires knowing what is already available publicly."[335] It is not clear that the intelligence community has thoroughly embraced an open source intelligence capability. Thus, it cannot honestly evaluate the efficiency of its activity if it cannot honestly compare the secret against what is already known. Even if it did one might reasonably expect that the secrecy and compartmentalisation culture might obfuscate such an investigation. However, to the great credit of key intelligence individuals within the

US military, such an initiative is being undertaken at US Special Operations Command (SOCOM) to establish precisely that.[336] In a 2005 'Memorandum for the Record' Steele states that: "The only truly successful DoD OSINT activity to date is the Special operations Command OSINT Branch, which answers 40 percent of SOCOM's all-source requirements at a cost of less than $1m a year".[337] With regard to Iraq prior to 2003 one might cynically but justly conclude that in the case of the US, with no Humint sources on the ground, and in the case of the UK, with five sources on the ground - three reliable but contradictory, one unreliable and one discredited[338] - that it should not take long to make the comparison with the plethora of open expertise that studied Iraq from Hans Blix's UN mission to David Kay's post-war survey group.

Intelligence as secret clandestine information gathering seems more suited to tactical puzzle solving while intelligence as open source exploitation is more suited to strategic mystery understanding. For example, the 1994 devaluation of the Mexican Peso was advertised well in advance by one analyst using open source information from Wall Street, and the 1998 Indian nuclear missile test had been openly proclaimed in the newspapers by the Indian BJP party throughout that year.[339] This is a deliberate generalisation rather than a rule as secret or open intelligence can achieve both tactical solution and strategic understanding to varying degrees.

The key point about understanding is that it is not solution with terminus but coping until the risk becomes tolerable.[340] The intelligence function cannot continue to solve puzzles in a Cold War mindset while failing to understand mysteries and manage the risks they present. Threats are a combination of capability and intent. However, threats also possess a risk that is measured by likelihood and impact.[341] In both the identification of the threat and the assessment of the risk they present, intelligence has come to err on capability almost ignoring the intent, likelihood and impact. During the Cold War, capability was all that the West needed to know and it would be matched. This static, stand-off arrangement no longer pertains.

The intractable problem of information sharing, technical, procedural and cultural, has dominated the intelligence community agenda in the US.[342] OSINT, while available as

an input to the all-source intelligence process for many years, has only in the last decade been formally exploited by the intelligence community as a discrete discipline. At best the application of OSINT in some intelligence agencies sees OSINT being accorded equivalent status alongside the other traditional, clandestine sources as a collection source in its own right. However, the literature is beginning to show that this equivalence may be at best patronising and at worst mistaken. Hulnick argues that OSINT contributes the basic building blocks for secret intelligence.[343] Taking this analogy a stage further, it may be that the model should show OSINT as the 'matrix'[344] in which all the other intelligence disciplines are set and directed, and against which they are benchmarked.[345] It may be that OSINT should be set free of the closed agencies altogether.[346] Perhaps as Mercado concludes, entirely discrete national OSINT capabilities should be established.[347] The 9/11 Commission did not go quite that far.[348]

Steele's literature and ideas for intelligence reform based upon OSINT, although seen from a US perspective, go some way to raise the profile of OSINT but they have found little traction in the US intelligence community.[349] By contrast in the Scandinavian countries or Canada, for example, OSINT has gained considerable traction. One reason might centre on the relative amounts of money available for national intelligence and the significantly greater cost of clandestine intelligence compared with open.

Berkowitz and Goodman also warn of intelligence becoming an irrelevance if it does not adapt to contemporary circumstances.[350] An early pointer to potential irrelevance occurred as far back as 1989 when the position of NATO Secretary General's Special Advisor on the Soviet Union was appointed from outside the traditional and dominant intelligence community to the director of an open source research organisation.[351] Interestingly, an appointment with similar parallels occurred in 2005, when Elliot Jardines was appointed Assistant Deputy Director National Intelligence for Open Source in the US from outside the traditional intelligence community. The subsequent decade and the first few years of the 21st century in particular have seen the proliferation of the information business into the private sector and wider security commons as the nature of risk diversifies beyond merely security. The Intelligence Community cannot

compete with this diversification; perhaps it should not attempt to, but it is being asked to do so in support of broader cross-governmental organisations such as the UK Civil Contingencies Secretariat and the US Department of Homeland Defense. Harnessing open source exploitation might enable the Intelligence Community to retain the position of principal and principled source of good intelligence on behalf of the nation.[352]

The traditional intelligence culture, pre-eminent in the Cold War, and still largely the prevailing culture today, does not fully acknowledge the value of OSINT because it is not equated with spying, secrecy and hardship in its obtaining.[353] Yet, intelligence professionals recognise that they are in the information business whatever its provenance.[354] Equally it is no defence to say that the volume of closed information is already so great that the additional volume derived from open source would simply swamp the process and therefore cannot be entertained. The data blizzard is certainly a challenge for intelligence but it is not new or peculiar to open sources.

In the real world, occupied by Anglo-Saxon intelligence communities at least, the resource employed in, and significance attached to, closed intelligence collection dominates open by a very considerable margin. Again the literature is extremely helpful in providing some very straightforward explanations as to why. The advent of the global digital age, from which contemporary open source opportunities have emerged, is still relatively new. The historical precedent, which has driven intelligence strategy to date, was fashioned by nearly 50 years of puzzle-solving engagement with a highly secretive, static, yet tangible adversary during the Cold War – curiously more like us than something 'other', and thus more fathomable than unfathomable. Many of that war's younger recruits are now intelligence's most senior leaders. The culture that they have fashioned is, inevitably, somewhat resistant to change. Interestingly, the resistance is more institutional than personal; in the fabric rather than the individual. Equally, the political machinations and emotional illiteracy within and between large bureaucratic organisations set up artificial and distracting objectives exemplified by turf wars, relative status anxieties, and budget protection mentalities. These drain their structures' energy and deviate them from their originating aims and purpose.

More instructively, recent intelligence-related inquiries have instigated a deliberative realignment of the principle security threat, such as it is to western nations at least (and this is itself hotly debated in a wider canon of non-intelligence literature), from a single clearly definable entity to a more amorphous and asymmetric one centred on terrorism, specifically Muslim extremism. This clear change in the nature of the security threat together with the specific findings of inquiry into the coordination of intelligence pre-9/11 have provided the impetus for an examination of intelligence change. Furthermore, the links between terrorism and other globally organised criminal activity - drugs, people-trafficking and arms smuggling - together with a perceived increasing repertoire of other risk agents - pandemics, natural disasters, and ecological catastrophe - have prompted discussion of a wider role for intelligence functions beyond merely security. This has a further knock-on effect for traditional intelligence communities in the sense that their customer base is also changing and broadening.

To date the clearest operationalisation of this strategic shift in intelligence community direction can be detected in two broad trends present on both sides of the Atlantic. First, the imposed change in intelligence credo from that of 'need to know' to that of 'need to share'. Second, an increasing importance attached to the role of analysis – absolutely, if not relatively to collection. Therefore, it is also unsurprising that, as the intelligence 'reform' debate has coalesced around a changing and broadening threat register, underpinned by a need to share information as well as incline more to analysis, the prominence of open source exploitation has increased proportionately. Indeed, the narrative and experience of this research reflects a similar path - beginning with clear disinterest and ending in invited participation.

2.4.10 OSINT, trust, and intelligence reform

Trust has been described as the basis of democracy. It is the safety net we construct for ourselves in order to bridge the gap between truth and uncertainty in an increasingly globalising and risk-perceptive world. O'Neill describes the placing of trust as a function of 'tests of trustworthiness': informed consent; expert judgement; and evidential examination.[355] However, these tests all still necessitate a degree of

assumption, choice, judgement, and not a little blind faith. They are not watertight. Indeed, trust cannot always be placed. Often we have to operate without guarantee.

By its very nature the intelligence function operates in a severe 'trustworthiness-testing' environment. Its product is then further examined by the same test criteria. In engineering terms this might be equated to an additional degree of inertia beyond normal complex systems. Yet, changing societal expectations are demanding ever-greater levels of trust in governments. Their intelligence functions, already engaging in reform to varying degrees, are no exception. Provided that societal expectations are rational, intelligence, including its necessary secret dimension, should pass the trustworthiness tests. It is not secret intelligence that is the enemy of trust; but the propensity to deceive and coerce wrapped up in a culture of secrecy.

Quite apart from the already recognised benefit of OSINT as intelligence source, OSINT potentially has something to contribute to trust and thus democracy. It can extend trust's safety net by revealing more evidence than institutions with legitimate security concerns might presently manage. It might contribute to reducing suspicion by increasing the opportunity for checking and questioning evidence, and thus at least countering the culture of cynicism if not actually any crisis of trust. It might reduce the urge to deceive by relieving the pressure and urge to classify information. Ultimately, it might bridge more of the gap between truth and uncertainty, thus placing intelligence in a better judgemental position of trustworthiness - not perfect, just better.

OSINT might also hinder the process. It is increasingly stated that the shear volume of fragmented, disparate information sources available to the open source specialist must speak to the veracity of the information.[356] Yet, volume does not imply credibility, just volume. Furthermore, sheer volume merely fragments and dissipates the opportunities for checking and questioning. It remains extant that checking the integrity of information and the trustworthiness of the informant is fundamental and yet not foolproof. Even then this will depend on the integrity and trustworthiness of those checking, and there is no complete answer to the eternal question: 'Who guards the guardians?'[357]

It should be no surprise then, that the intelligence community is wary of wholeheartedly endorsing the exploitation of open sources of information. In the same sense, that the author has argued elsewhere, it is similarly wary of engaging in wholesale intelligence reform, incorporating a completely new set of ethics, or simply abandoning long developed principles and frameworks. The benefits or otherwise have to be demonstrable, while pressure for change from a publicly communicated yet evidentially weak amorphous clamour is resisted in the absence of strong argument.

Nevertheless, the raft of inquiries post 9/11 and Iraq 2003 have collectively articulated the necessity for a degree of evolution and transformation in the nature of the conduct of intelligence activity. Whether the inquiries persuade us that the earliest years of the 21st century demonstrated either, a failing in, or, a politicisation of, the intelligence process is a debate that will likely run and run. Regardless, intelligence failure and intelligence politicisation are not new phenomena - they both have historical precedent.

Since 9/11 much has been said about the 'failure of intelligence'. The discussion of intelligence failure is nothing new; but events of the 21st century, coupled with the 'media effect' of the 1990s, have catapulted the issue into the forefront of public debate. The 'western' intelligence mechanism, resurrected in WWI, refined in WWII and honed by the Cold War, is now considered by many of its senior practitioners to be a poor fit for contemporary society. If OSINT is a potential lifeline for re-aligning intelligence practice with contemporary society then its treatment should be part of the wider reform debate to explain why.

2.5 Incomplete: The literature's understanding of OSINT's contribution

The changing contemporary setting for the conduct of intelligence has spawned a burgeoning literature debate on intelligence reform. However, inquiries into failure or politicisation aside, the root driver of meaningful change today is a recognition that the Cold War mentality of secret intelligence is at odds with an ICT transformation creating ever more open sources of information. Contextually this transformation is also partly

responsible for raising and changing the risk profile that nation-states face, as well as changing societal expectations of, and trust in, their governing institutions.

The reform debate in the literature partly reflects these changing circumstances. Concepts such as openness, transparency, scrutiny, disclosure and trust are regularly contrasted positively against secrecy, classification and compartmentalisation. The literature on reform is by and large unanimously in favour of some type of reform that reflects changing threats, changing ICT capabilities, and changing societies. The incumbent practitioners, with access to the current intelligence picture, continue to caution against abandoning the security principal in this often-dangerous activity. Yet, they too are engaging in the debate.

Indeed, it would be curious to think that organisations should not adapt in response to a changing environment. Many intelligence organisations are already responding and incorporating new sources, methods, technologies and even philosophies appropriate to the contemporary forces of change. One such is the formal exploitation of open sources of information. However, the debate surrounding where and how open sources should be exploited, rather than why, tends to dominate; and it is politically, culturally and structurally driven rather than purposefully.[358] The 'why' remains to be determined.

2.5.1 The 'issues' of open source exploitation

In a recent paper (2007), albeit US-centric, Bean summarises much of the pertinent literature and raises several key issues for the exploitation of open source.[359] First, he argues that the entire subject of OSINT is being used as an object of political posturing by the US intelligence community as they try to organise and shape resource, funding, structure, location, and leadership for their own individual or organisational ends. In this regard, he suggests that the creation of the OSC is as much rhetoric as it is fundamental change, given that resource input is diminished by output, and organisation is designed to be a service to the community rather than a 'one-stop' shop for OSINT. Second, that OSINT remains contested between 'discrete discipline' and 'foundational

base', further reflecting the procedural conundrum of open source; should it be a decentralised and distributed affair or a centralised and controlled one. Third, that additional contestation occurs as to whether open source information is 'collected', 'acquired', or 'obtained'. These different descriptions are loaded for the US community. Collection implies a discrete intelligence discipline and in the US still causes concern for domestic intelligence activity. Acquisition suggests that someone else has done the collection and that open source is merely a 'second-hand' effort. This is implicitly perceived as less contentious and of course cheaper. Obtaining open source information is a compromise expressed by the Director of the US Open Source Center in an effort to find the right word.[360] Fourth, there is considerable debate over the appropriate location of open source exploitation: public or private sector; centralised or distributed. There is a commercial mismatch between the public sector's desire to 'pay for it once and once only' and the private sector's desire to 'do it once and sell it many times'. This reflects the public sector desire to organise centrally for cost-cutting and efficiency purposes, if nothing else, versus, the private sector's fragmented and disparate concentration of subject matter expertise. Furthermore, there is a philosophical gulf between their notions of effectiveness. The private sector can simply address effectiveness through the concept of value-added to the bottom-line. The public sector has to address the contribution to security, which is significantly less susceptible to metrics. Finally, for the public-private divide, there is an epistemological gulf between the appropriate forms of validation for information sources. The public sector demands thoroughly traceable and referenced sources. The private sector considers itself to represent expertise and thus guarantors of provenance. Thus, the public sector default to a quality argument, while the private sector tend towards utility.

These dichotomies seem more pronounced in the US community where, perhaps, scale and culture dictate that they will always be present. However, they are also noted in the data collection phase (Chapter Four) of this research and are addressed in the analysis (Chapter Five) and conclusion (Chapter Six) chapters. Bean acknowledges that most of these dichotomies remain unanswered and contentious. He concludes that a fundamental question remains: "What constitutes OSINT and how is it distinguished

from other types of intelligence and information?"[361] This research attempts to answer that question.

2.5.2 The literature's 'description' of the contribution of open source exploitation

> "According to many policymakers and government officials, United States national security may depend on OSINT. Yet, a fundamental question remains: what constitutes OSINT and how is it distinguished from other types of intelligence and information?"
>
> Hamilton Bean, 2007[362]

Literature commenting upon the 'value' or contribution of open source exploitation is also not new, but significantly more rare. In a, then secret, briefing to the CIA in 1969 (declassified in 1997) Croom summarised much of the debate, the potential benefits, and key policy issue (resource allocation) surrounding open source exploitation in just seven well-crafted pages.[363] However, despite recognising 'utility' and the possibility of 'focusing' closed intelligence as a result of open, he does not explicitly recognise other contributing factors of OSINT that other literature and this research establish.

Thus, two further authors are worth noting as the start point for this research, because they discern some similar and some divergent qualities of OSINT. First, Mercado specifically lists 'speed', 'quantity', 'quality', 'clarity', 'ease of use', and 'cost' as being key contributors to the intelligence function in relation to closed or clandestine secrets.[364] Speed, quantity and cost might usefully be collated into one contributing factor - 'utility'. Clarity and ease of use might also be collated and reinterpreted as 'communicability'. Unfortunately, Mercado's treatment is a brief one, albeit based upon the author's professional experience, but with no supporting evidence.[365] Second, Sands (in Sims and Gerber) in a more comprehensive treatment of OSINT articulates five contributing factors that open sources offer relative to closed: 'assessment frame of reference'; 'protection' of closed material; 'credibility'; 'ready access'; 'enhanced assessment methodology'.[366] These attributes are more nuanced than Mercado's and are reflected throughout this research, where frame of reference is initially reinterpreted as 'matrix' and finally in Chapter Five absorbed into a broader notion of 'context'. Protection is treated as part of the notion of 'communicability', and ready access as

utility. Assessment methodology is initially discounted as an attribute of open source exploitation, rather it is perceived as something more appropriate to intelligence as a whole. However, the data in Chapter Four indicates that open source exploitation does have something to contribute in its own right to assessment, and is recognised by the notion of 'analysis' in the final model. Credibility is discounted as being a specifically open source attribute. Credibility is a desirable quality of all information whether it is closed or openly derived. While Sands' piece is more nuanced, and incorporates more supporting evidence, there remains no exposition of any deliberate research into the contribution of open source exploitation to the intelligence function in terms of how and why.

When combined with the practitioner literature, five broad attributes of OSINT begin to emerge that are 'claimed' for it in comparison to closed. Collectively they represent a working hypothesis and departure point for this research. Chapter Four shows how the research modifies these attributes, derives additional ones to form a more comprehensive model of high order factors describing open source's contribution, and finally tests it. For now, they can be summarised here as: 'matrix', 'surge', 'revelation', 'utility'; and 'horizon-scanning':

- **Matrix.** Rather than sit alongside the other traditional intelligence disciplines, OSINT might form the matrix in which the other intelligence disciplines are placed. In this manner, OSINT can become a driver and focuser of the closed intelligence disciplines, providing context, corroboration and queuing.

- **Surge.** OSINT can confer a surge capability. When a new risk is identified about which little is known but much needs to be acquired and fast, exploiting open sources is one way of building capacity quickly.

- **Revelation.** OSINT can be used to reveal knowledge of areas of interest, where traditional sources are simply not represented, unavailable or not warranted. A very bright light can be shone into very dark areas that ordinarily would not or could not be covered. Additionally, revelation can also be taken to mean the notion of

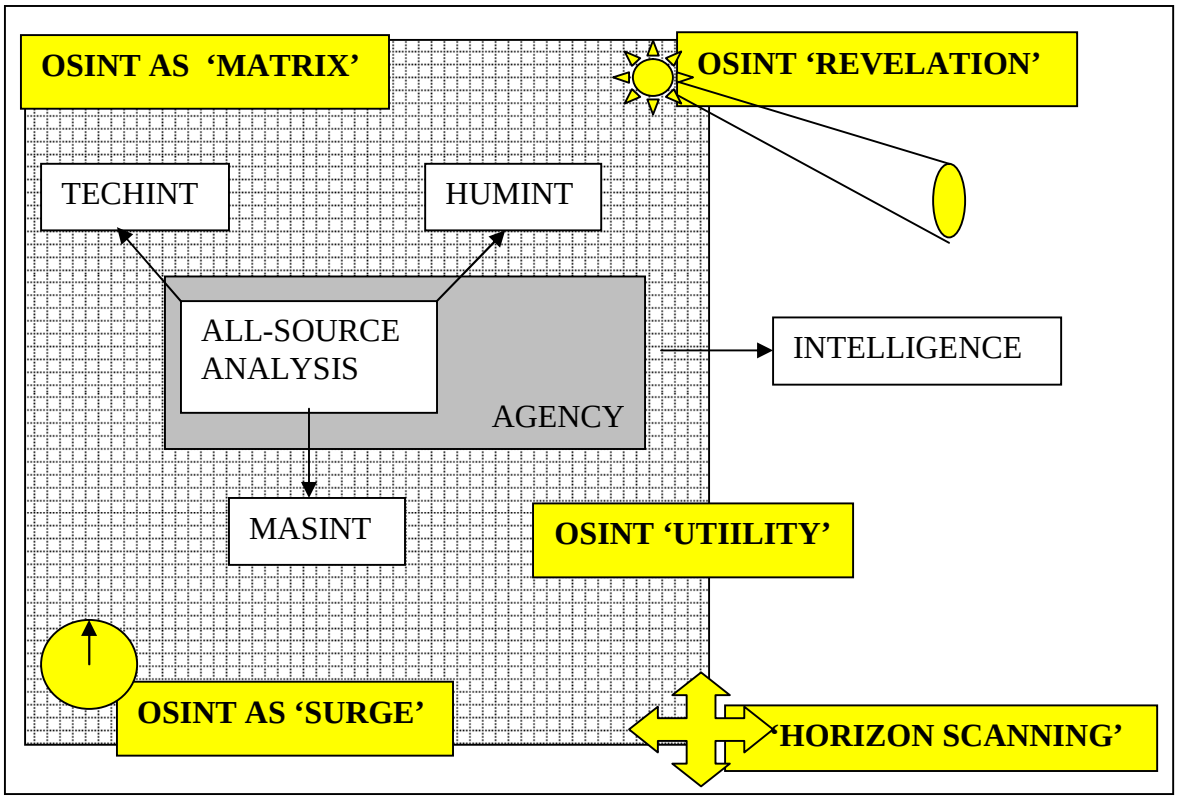
revealing information internal or external to the intelligence community that security implication might otherwise prevent, and thus has a powerful effect in terms of communication. These two descriptions do not sit comfortably together and are split out as the model is developed.

- **Utility**. The speed, volume and cost of OSINT are highly favourable characteristics in comparison to closed collection. It can be more quickly launched or redirected. It can produce vast amounts of information and it is considerably cheaper to undertake. Steele cites a challenge to the US Government's intelligence community, which serves as example.[367] He infers that it seems wasteful if not negligent to concentrate expensive and sensitive resources on targets that can be achieved by cheaper, more capable and less vulnerable means.[368] Yet, the case-studies examined in this research all operate on relatively small budgets while often contributing valuable returns. Their return on investment seems comparatively high although no such comparison between the Intelligence disciplines is clearly undertaken.

- **Horizon-scanning.** The traditional intelligence disciplines are requirements driven. That is to say, questions are asked of them and they respond. Analysis by virtue of hypothesising creates alternative scenarios for testing and makes assumptions about their hypotheses. The hypotheses and findings can create further requirements but nowhere in this model does scanning for new risk take place. As Berkowitz and Goodman note, intelligence can no longer complacently watch threats, it must actively look for the rapidly emerging and mutating threats of contemporary society.[369] Open source might be better positioned to contribute to that effort.

The factors identified in the literature might usefully be represented in Figure 2.5 below.

Figure 2.5: The literature's view



Source: Author

Both Drucker's and Steele's remarks at the beginning of the chapter are thus pertinent to this thesis. Is the exploitation of OSINT changing the nature of the intelligence institution? If so, how, why and what are the implications? Despite the contributing factors observable from the literature, the fact remains that there is no literature that the author has discovered, which sets out to deliberately identify the 'benefits' of open source exploitation through research into how and why intelligence agencies exploit open source information.

2.6 Summary: Minding the gap

The review of literature reveals two key phenomena pertinent to this research. First, contemporary context is shaping the conduct of intelligence as much as it is shaping the subject matter for intelligence. Second, the exploitation of open sources of information, an example of that changing conduct of intelligence, is scarcely treated.

The literature reflects much of the debate about the contemporary intelligence function: the definition of intelligence is perceived broken; the long-established model for its conduct - the intelligence cycle - is not realistically representative of the intelligence process; on the one hand, there is cultural and organisational reluctance to move from the prominence afforded secret intelligence to an engagement with the total information business;[370] and on the other, as Johnston indicates, certainly in regard to analysis, there is a community-wide expression and desire for change. He further suggests that the logjam resides at the political and institutional level: an unwillingness to admit 'failure'; an unwillingness to assess performance; and an unwillingness to engage in the notion of openness.[371]

While definitions of intelligence, models of its process, constituents of its community, and recipients of its product are all being 'rewritten' in the discussion surrounding intelligence reform, there is actually little new in the nature of intelligence in the sense of its purpose. It remains a supporting function to decision and policy-makers. Much of what is perceived new is, more accurately, to do with its conduct rather than its purpose, and much of that is merely new to 'us'.

However, what is different in contemporary times is the context in which intelligence functions. Significant geo-political and socio-cultural influences are shaping it and our response to it. The literature has suggested to the author that three such influences are significant: globalisation; risk society; and changing societal expectations. Underpinning these influences is a thoroughly pervasive transformation in ICT. In this regard the conduct of intelligence, in the sense of how it achieves its purpose is changing in order to utilise this ICT transformation.

The exploitation of open sources of information is considered to be one such manifestation. Yet, the contribution of open sources to a modern intelligence capability has been noted and highly rated for 60 years at least. A clear consensus amongst intelligence practitioners broadly assesses that OSINT constitutes a significant proportion of final intelligence product; probably 80 percent, and possibly as much as 95 percent for certain intelligence requirements. However, regardless of the

authenticity of the derivation of that figure, this ‘percentage contribution’ cant is also misleading, representing as it does a measure of efficiency rather than effectiveness. In a decision and action oriented discipline, it is not so much a question of how efficient open source exploitation can be. Rather, it is more pertinent to understand its effectiveness - what it can do. Having understood effectiveness, then it might be more logical and persuasive to revisit efficiency in terms of policy and resource allocation. Regrettably, as with so many disciplines of contemporary society that engage in the management of uncertainty, the proof or demonstration of effectiveness is highly subjective, largely immeasurable, and deeply intractable. Unfortunately, these contra-indications do not seem to stop the attempt.

This chapter has begun the process of describing how open source is perceived effective within a broader intelligence function. The literature regarding the exploitation of open sources is sparse or somewhat idiosyncratic. The claimed benefits of open source exploitation are unsupported, explaining neither why nor how it might be efficacious to the broader intelligence effort. The little literature directed at such an explanation can be summarised by the descriptors: matrix; surge; revelation; utility; and horizon-scanning. But, these descriptors betray a paucity of evidence and a significant knowledge gap, which this research now goes on to fill. Yet, they also represent a useful working hypothesis and start-point for this research effort: to develop and test a more sophisticated model that describes the contribution of open source exploitation against existing intelligence community practice.

References and Notes:

[1] Drucker, P.F., 'The Next Information Revolution', *Forbes ASAP*, 24 August 1998, p.46.

[2] Steele, R.D., 2002, *The New Craft of Intelligence: Personal, Public and Political*, Oakton, Virginia: OSS International Press, p.43.

[3] Aldrich, R.J., 2005, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, 16, 2005, pp.73-88.

[4] Robert David Steele's work can be viewed at http://www.oss.net

[5] These include: Holden-Rhodes, J.F., 1997, *Sharing the Secrets: Open Source Intelligence and the War on Drugs*, West Port, CT: Praeger; Lowenthal, M.M., 1999, 'Open Source Intelligence: New Myths, New Realities', *Intelligencer*, 10, 1, pp.7-9; Hulnick, A.S., 2002, 'The Downside of Open Source Intelligence', *International Journal of Intelligence and CounterIntelligence*, 15, 4, pp.565-579; Clift, A.D., 2003, 'From Semaphore to Predator: Intelligence in the Internet Era', *Studies in Intelligence*, 47, 3; Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press, pp.93-136; Mercado, S., 2004, 'A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence: Journal of the American Intelligence Professional*, 48, 3, pp.45-55; Mercado, S.C., 2001, 'Open Source Intelligence from the Airwaves: FBIS Against the Axis', 1941-1945, *Studies in Intelligence*, Fall-Winter, 11; Pringle, R.W., 2003, 'The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989', *International Journal of Intelligence and CounterIntelligence*, 16, pp.280-289; Reese, D.A., 2005, '50 Years of Excellence: ASD Forges Ahead as the Army's Premier OSINT Unit in the Pacific', *Military Intelligence Professional Bulletin*, 31, 4, pp.27-29; Bean, H., 2007, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and CounterIntelligence*, 20, 2, pp.240-257.

[6] Croom, H.L., 1969, 'The Exploitation of Foreign Open Sources', *Studies in Intelligence*, 13, 2, (Summer), pp.129-136; Mercado, S.C., 2005, 'Reexamining the Distinction Between Open Information and Secrets', *Studies in Intelligence*, 49, 2; Sands, A., 2005, 'Integrating Open Sources into Transnational Threat Assessments', in: Sims, J.E., Gerber, Burton., (Eds), 2005, *Transforming US Intelligence*, Washington, DC.: Georgetown University Press, pp.63-78.

[7] Rischard, J.F., 2002, *High Noon: 20 Global Issues, 20 Years to Solve Them*, Oxford: Perseus Press.

[8] Weller, G.R., 2001, 'The Internal Modernization of Western Intelligence Agencies', *International Journal of Intelligence and CounterIntelligence*, 14, 3, pp.299-322.

[9] Gibson, S.D., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22.

[10] Mercado, S., 2004, 'A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence*, 48, 3, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol48no3/article05.html

[11] Laqueur, W., 1985, *A World of Secrets: The Uses and Limits of Intelligence*, New York: Basic Books, p.8.

[12] Kent, S., 1966, *Strategic Intelligence for American World Policy*, Princeton, NJ: Princeton University; Lowenthal, M.M., 2003, *Intelligence: From Secrets to Policy*, Washington: CQ Press; Goodman, M., 2006, 'Studying and Teaching about Intelligence: The Approach in the United Kingdom', *Studies in Intelligence*, 50, 2, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no2/html_files/Studying_Teaching_6.htm

[13] Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press, pp.1-8.

[14] Michael Warner was the CIA's chief archivist when he compiled the definition. He subsequently became Historian for the Office of Director of National Intelligence in 2005.

[15] Warner, M., 2002, 'Wanted: A Definition of Intelligence', *Studies in Intelligence*, 46, 3, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v46i3a02p.htm

[16] Warner, M., 2006, 'The Divine Skein: Sun Tzu on Intelligence', *Intelligence and National Security*, 21, 4, pp.483-492.

[17] Gill, P., Phythian, M., 2006, *op cit*, p.7.

[18] Johnston, R., 2005, *Analytic Culture in the U.S. Intelligence Community*, Washington DC: Center for the Study of Intelligence, Central Intelligence Agency, p.4.

[19] Keegan, J., 2003, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, London: Pimlico. Pimlico edition 2004, p.20.

[20] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press; Berkowitz, B.D., Goodman, A.E., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press; Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger.

[21] Wilson, P., 2005, 'The Contribution of Intelligence Services to Security Sector Reform', *Conflict, Security and Development*, 5, 1, pp.87-107, and in correspondence with author.

[22] Omand, D., 2007, 'Reflections on Secret Intelligence' in: Hennessy, P., 2007 (Ed), The New Protective State: Government, Intelligence and Terrorism, London: Continuum Books, p.99.

[23] *Ibid*, p.100.

[24] Herman, M., 2001, *Intelligence Services in the Information Age*, London: Frank Cass.

[25] Odom, W., 2003, *Fixing Intelligence for a More Secure America*, New Haven: Yale.

[26] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[27] *Ibid.*

[28] Herman, M., 2001, *Intelligence Services in the Information Age*, London: Frank Cass; Bruneau, T.C., 2001, 'Controlling Intelligence in New Democracies', *International Journal of Intelligence and CounterIntelligence*, 14, 3, pp.323-341.

[29] I am grateful to Dr Philip Davies, Deputy Director at the Brunel Centre for Intelligence & Security Studies, for pointing out that this 'axis' is often referred to as the 'Anglo-Saxon' division by those observing it from outside.

[30] Chris Donnelly points out that post Cold War the Former Soviet Union and its satellites developed four distinct brands of intelligence doctrine; Russian/Ukrainian, Central European & Baltic States, Czechoslovakia and East Germany (no longer constituted as such), and the rest. They display variety along the spectrum between tool of the State to State tool.

[31] Shulsky, A.N., Schmitt, G J., 2002, *Silent Warfare: Understanding the World of Intelligence*, Dulles: Brassey's, Inc.

[32] Johnson, L., 2003, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, 22, 1, pp.1-28.

[33] US Army, 2004, US Army Field Manual - Intelligence 2-0.

[34] Hulnick, A.S., 2004, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Westport, CT: Praeger, p.13.

[35] Wilson, P., 2005, *op cit.*

[36] *Ibid.*

[37] Young, D., 2006, in: 'Spies, Lies & Intelligence: A Briefing Book', prepared for the Christ Church College 'Conflict' Conference, Oxford 5-8 September 2006, by Oxford Analytica, Oxford.

[38] Johnson, L., 2003, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, 22, 1, pp.1-28.

[39] Hulnick, A.S., 2006, 'What's Wrong with the Intelligence Cycle', *Intelligence and National Security*, 21, 6, pp.959-979.

[40] UK Intelligence and Security Committee, 2004, Annual Report 2003-2004, Report No: Cm 6240, 2004/06/29.

[41] Krizan, L., 1999, Number 6 , *Intelligence Essentials for Everyone*, US Joint Military Intelligence College, Washington DC.

[42] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press; Berkowitz, B.D., Goodman, A.E., 2000, *op cit*; Lowenthal, M.M., 2003, *op cit*.

[43] Johnston, R., 2005, *op cit*, pp.45-57 (the complex diagram of the model is on p.52 of this reference).

[44] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press, p.106.

[45] Johnston, R., 2005, *op cit*, pp.45-57.

[46] Hulnick, A.S., 1999, 'Openness: Being Public About Secret Intelligence', *International Journal of Intelligence and CounterIntelligence*, 12, 4, pp.463-483; Johnson, L., 2003, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, 22, 1, pp.1-28.

[47] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press; Berkowitz, B.D., Goodman, A.E., 2000, *op cit*.

[48] Private conversation with Dr Jacob Kipp; Wilson, P., 2005, *op cit;* the author's own experience documented in Gibson, S.D., 1997, *The Last Mission Behind the Iron Curtain*, Stroud: Sutton. For a wider discussion of the significant role that uncertainty and chance play in organisations, see for example:

Ormerod, P., 2005, *Why Most Things Fail: Evolution, Extinction and Economics*, London: Faber and Faber; Power, M., 2007, *Organized Uncertainty: Designing a World of Risk Management*, Oxford: Oxford University Press; Taleb, N.N., 2004, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, London: Penguin Books.

[49] US Department of Defense Joint Chiefs of Staff, 2004, *Joint and National Intelligence Support to Military Operations*, JP 2-01, p.III-2.

[50] *Ibid*, p.xv in comparison to p.GL-17.

[51] Steele, R.D., 1996, 'Creating a Smart Nation: Strategy, Policy, Intelligence, and Information', *Government Information Quarterly*, 13, 2, pp.159-173.

[52] Steele, R.D., 2002, *The New Craft of Intelligence Personal, Public, & Political*, Oakton, Virginia: OSS International Press.

[53] Gibson, S.D., 1997, *op cit.*

[54] Florini, A., (Ed), 2000, *The Third Force: The Rise of Transnational Civil Society*, Washington: Carnegie Endowment for International Peace.

[55] Aldrich, R.J., 2005, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, 16, 2005, pp.73-88.

[56] US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company.

[57] BBC News – New Unit Targets Net Paedophiles dated 24 April 2006 at: http://news.bbc.co.uk/1/hi/uk/4937264.stm

[58] Warren, M.E., (Ed), 1999, *Democracy and Trust*, Cambridge: Cambridge University Press.

[59] O'Neill, O., 2002, *A Question of Trust: The BBC Reith Lectures 2002*, Cambridge: Cambridge University Press.

[60] De Jong, B., Platje, W., Steele, R.D., (Eds), 2003, *Peacekeeping Intelligence: Emerging Concepts for the Future*, Oakton, Virginia: OSS International Press.

[61] Evolution rather than revolution in intelligence affairs is advocated by intelligence practitioners as diverse as Sir David Omand in a presentation to the Oxford Intelligence Group in 2005, and the Director of SOCOM's Open Source Exploitation Branch, in: Interview, 2006, SOCOM 1, 18-120 April 2006.

[62] Sardar, Z., Wyn-Davies, M., 2002, *Why Do People Hate America?*, Cambridge: Icon Books.

[63] O'Hara, K., 2004, *Trust: From Socrates to Spin*, Cambridge: Icon Books.

[64] *Ibid.*

[65] Held, D., McGrew, A., 2003, *Globalization/Anti-Globalization*, Malden, MA: Polity Press; Held, D., McGrew, A., 2002, *Governing Globalization: Power, Authority and Global Governance*, Malden: Blackwell Publishing; Florini, A., 2003, *The Coming Democracy: New Rules for Running a New World Order*, Washington: Island Press; Florini, A., (Ed), 2000, *op cit;* Rischard, J.F., 2002, *op cit.*

[66] Stiglitz, J., 2002, *Globalization and its Discontents*, London: Penguin.

[67] Knightley, P., 2003, *The Second Oldest Profession: Spies and Spying in the Twentieth Century*, London: Pimlico; Goodman, M.A., '2003, 9/11: The Failure of Strategic Intelligence', *Intelligence and*

National Security, 18, 4, pp.59-71; Treverton, G.F., 2003, 'Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons', *Intelligence and National Security*, 18, 4, pp.121-140.

[68] Tussing, B.B., 2003, *Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process and Culture* - a private communication with author.

[69] UK government speaker at a joint meeting of the Oxford Intelligence Group and the Reuters Foundation, Osloer McGovern Centre, 13 December 2004, conducted under Chatham House Rules.

[70] Conversation with the director of EUROPOL's counter-terrorist intelligence section Nov 2002.

[71] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*, pp.74-98.

[72] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press; Odom, W., 2003, *Fixing Intelligence for a More Secure America*, New Haven: Yale; Dupont, A., 2003, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, 18, 4, pp.15-39; Wark, W.K., 2003, 'Learning to Live With Intelligence', *Intelligence and National Security*, 18, 4, pp.1-14; Goodman, M.A., 2003, *op cit;* Deibert, R.J., 2003, 'Deep Probe: The Evolution of Network Intelligence', *Intelligence and National Security*, 18, 4, pp.175-193; Berkowitz, B.D., Goodman, A.E., 2000, *op cit*.

[73] US Senate Committee on Governmental Affairs, 2004, Summary of Intelligence Reform and Terrorism Prevention Act of 2004, US Senate, 2004/12/06, available at: http://www.fas.org/irp/congress/2004_rpt/s2845-summ.pdf (9 December 2004).

[74] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*.

[75] Lowenthal, M.M., 2003, *op cit.*

[76] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*, p.80.

[77] Walley, A., 1938, *The Analects of Confucius*, xii, 7, p. 164 as cited in O'Neill, O., 2002, *op cit*.

[78] Cornyn, J., 2004, 'Ensuring the Consent of the Governed', *LBJ Journal of Public Affairs*, Fall, p.7-10.

[79] As quoted in: Cornyn, J., 2004, 'Ensuring the Consent of the Governed: America's Commitment to Freedom of Information and Openness in Government', *Lyndon B. Johnson Journal of PublicAffairs*, 17, 1, p.8.

[80] O' Neill, O., 2006, 'Transparency and the Ethics of Communication', in Hood, C., Heald, D., 2006, *Transparency: The Key to Better Governance?*, Oxford: Oxford University Press, pp.75-90.

[81] Heald, D., 2006, 'Transparency as an Instrumental Value', in Hood, C., Heald, D., 2006, *op cit*, pp.59-74.

[82] Friedman, R.S., 1998, 'Open Source Intelligence', *Parameters*, Summer, 159-165.

[83] Atlee, T., 2003, *The Tao of Democracy*, Cranston: The Writers' Collective; Sardar, Z., Wyn-Davies, M., 2002, *op cit;* Held, D., McGrew, A., 2003, *op cit;* Held, D., McGrew, A., 2002, *op cit.*

[84] Aldrich, R., 2006, presentation to *Spies, Lies & Intelligence*, Christ Church College 'Conflict' Conference, Oxford 5-8 September 2006.

[85] Rischard, J.F., 2002, *op cit.*

[86] Gray, C.S., 2005, *Another Bloody Century: Future Warfare*, London: Weidenfeld & Nicholson, pp.67-69.

[87] Friedman, R.S., 1998, *op cit.*

[88] The UK FOIA came into full force in January 2005.

[89] Roberts, A., 2006, 'Dashed Expectation: Governmental Adaptation to Transparency Rules', in Hood, C., Heald, D., 2006, *op cit,* pp.107-125.

[90] The US FOIA has a complimentary opt out Act for CIA operational activity (The CIA Information Act 1984).

[91] Aftergood, S., Secrecy News, 28 October 2004, available at: http://www.fas.org/sgp/foia The US reluctance to disclose the intelligence budget was reinforced by the US Intelligence Reform and Terrorism Prevention Act of 2004.

[92] Aftergood, S., Secrecy News, 7 November 2005, available at: http://www.fas.org/sgp/foia

[93] The 1988 beginning of the final unravelling of East European Soviet satellite states was at least viewed if not actually hastened through 1989 as a result of the ability of their populations to receive some satellite television and some considerable terrestrial television. In earlier years the author was able to note first-hand that many terrestrial television aerials pointed west where they coincided with the boundaries of western television broadcast.

[94] Held, D., McGrew, A., 2002, *op cit.*

[95] There are some notable exceptions: The 1987 Montreal Protocol on ozone depletion; the 1997 Ottawa Treaty to ban land-mines; and the establishment of Transparency International to report on global corruption in the 1990s.

[96] Chomsky, N., 2004, *Hegemony or Survival: America's Quest for Global Dominance*, London: Penguin.

[97] Rees, M., 2003, *Our Final Century: Will the Human Race Survive the Twenty-First Century*, London: William Heinemann.

[98] Florini, A., 2003, *op cit.*

[99] O'Neill, O., 2002, *op cit*, p.16.

[100] Furedi, F., 2002, *Culture of Fear: Risk-Taking and the Morality of Low Expectation*, London: Continuum.

[101] Furedi, F., 2004, *Therapy Culture: Cultivating Vulnerability in an Uncertain Age*, London: Routledge.

[102] Bryson, B., 2004, *A Short History of Nearly Everything*, London: Doubleday; Rees, M., 2003, *op cit;* Fukuyama, F., 2002, *Our Posthuman Future*, London: Profile Books; Angell, I., 2000, *The New Barbarian Manifesto: How to Survive the Information Age*, London: Kogan Page; Joy, B., 2000, 'Why the Future Doesn't Need Us', *Wired Magazine*, 1 April 2000.

[103] Durodié, W., 2003, 'Limitations of Public Dialogue in Science and the rise of New 'Experts'', *Critical Review of International Social and Political Philosophy*, 6, 4, pp.82-92.

[104] Gibson, S.D., 2004, 'Risk Management: Where Safety and Security Diverge', *Journal of the International Society for Respiratory Protection*, 21, Spring-Summer, pp.40-48.

[105] Power, M., 2004, *The Risk Management of Everything*, London: Demos; Power, M., 1994, *The Audit Explosion*, London.

[106] Power, M., 2007, *op cit*.

[107] Beck, U., 1999, *World Risk Society*, Oxford: Blackwell.

[108] Jeffreys-Jones alludes to this in his description of the expansion of intelligence as a confidence trick perpetrated as a result of fear on the back of 9/11. See: Jeffreys-Jones, R., 2003, *Cloak and Dollar: A History of American Secret Intelligence*, London: Yale University Press, p. xviii.

[109] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[110] Flavin, C., 2004, WorldWatch Institute - President's Annual Address, 7 Dec 04, available at: http://www.worldwatch.org

[111] Rischard, J.F., 2002, *op cit.*

[112] Hulnick, A.S., 2004, *op cit*, p.22.

[113] Devji, F., 2005, *Landscapes of the Jihad*, London: Hurst & Co.

[114] Sagan, C., 1994, *Pale Blue Dot: A Vision of the Human Future in Space*, New York: Random House.

[115] Chomsky, N., 2004, *op cit.*

[116] The US DoD budget in 2002 was $344 Bn [*Source:* White House Office of Management and Budget]. The US aid budget in 2003 was $39.29 Bn [*Source:* US Department of State. International Affairs (Function 150) Budget request].

[117] Every day approximately 3,000 people die worldwide as a result of road accidents [*Source:* UN WHO/World Bank Joint Report 'World Report on Road Traffic Injury Prevention' 7 April 2004].
In the USA approximately 29,000 people die by firearms annually [*Source:* Centers for Disease Control and Prevention, *National Vital Statistics Reports,* vol. 50, no. 15, Sept. 16, 2002]; The RAND-MIPT terrorism database records 11,810 fatalities from terrorism between 1997 and 2003 inclusive, available at: http://www.tkb.org/

[118] Klinke, A., Renn, O., 2002, 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies', *Risk Analysis: An International Journal*, 22, 6, pp.1071-1094.

[119] Atlee, T., 2003, *op cit.* Atlee deliberately uses 'xx' for emphasis and distinction.

[120] Ormerod, P., 2005, *Why Most Things Fail: Evolution, Extinction and Economics*, London, pp.17-35.

[121] *Ibid*, p.98.

[122] Gray, J., 1998, *False Dawn: The Delusions of Global Capitalism*, London: Granta Books.

[123] O'Hara, K., 2004, *op cit.*

[124] Taleb, N.N., 2004, *op cit*; Taleb, N.N., 2007, *The Black Swan: The Impact of the Highly Improbable*, London: Penguin Books.

[125] Ormerod, P., 2005, *op cit*, p.239.

[126] Maddison, A. *Monitoring the World Economy 1820-1992*, cited and modified by Ormerod (for data to 2004) in Ormerod, P., 2005, *op cit*, p.47. This finding has been most recently confirmed by the UK-based Joseph Rowntree Foundation report, *Poverty and Wealth Across Britain1968 to 2005* of July 2007, available at: http://www.jrf.org.uk/knowledge/findings/housing/2077.asp

[127] Ormerod, P., 2005, *op cit*, p.39.

[128] Ormerod, P., 2005, *op cit*, pp.58-76.

[129] Atlee, T., 2003, *op cit;* Klinke, A., Renn, O., 2002, *op cit;* Adams, J., 1995, *Risk*, London: UCL Press; Slovic, P., 2000, *The Perception of Risk*, London: Earthscan.

[130] Treverton, G.F., 2003, Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons, *Intelligence and National Security*, 18, 4, pp.121-140; Dupont, A., 2003, *op cit.*

[131] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[132] Taleb, N.N., 2004, *op cit*, p.146.

[133] Collis, J., Hussey, R., 2003, *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, (Second Edition), New York: Palgrave Macmillan.

[134] Nye, J.S., Jr., 2004, *Soft Power: The Means to Success in World Politics*, Cambridge (MA): Public Affairs.

[135] Hennessy, P., 2007, *The New Protective State: Government, Intelligence and Terrorism*, London: Continuum; Treverton, G.F., 2003, Terrorism, 'Intelligence and Law Enforcement: Learning the Right Lessons', *Intelligence and National Security*, 18, 4, pp.121-140; Berkowitz, B.D., Goodman, A.E., 2000, *op cit*; Hulnick, A.S., 1999, 'Openness: Being Public About Secret Intelligence', *International Journal of Intelligence and CounterIntelligence*, 12, 4, pp.463-483.

[136] Seaquist, L., 2004, 'Intelligence for Grownups', *Christian Science Monitor*: 6 December, 2004, available at: http://www.csmonitor.com/2004/1206/p09s02-coop.htm (9 December 2004).

[137] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663, p.647.

[138] Giddens, A., 2002, *Runaway World: How Globalisation is Reshaping Our Lives*, London: Profile Books.

[139] _____ 2005, 'Out of the Darkness', *The Economist*, 1 January 2005, p.19.

[140] O'Hara, K., 2004, *op cit.*

[141] Power, M., 2004, *op cit;* Hunt, B., 2004, *The Timid Corporation: Why Business is Terrified of Taking Risk*, London: Wiley.

[142] Politi, A., 2003, 'The Citizen as "Intelligence Minuteman"', *International Journal of Intelligence and CounterIntelligence*, 16, pp.34-38.

[143] Davis, I., 2005, 'The Biggest Contract', *The Economist*, 28 May 2005, pp.87-89.

[144] *Ibid.*

[145] Reynolds, G., 2006, *An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government and Other Goliaths*, Nashville (TE): Nelson Current; Surowiecki, J., 2004, *The Wisdom of Crowds*, London: Little Brown.

[146] Scoble, R., Israel, S, 2006, *Naked Conversations: How Blogs are Changing the Way Businesses Talk with Customers*, Hoboken (NJ): John Wiley & Sons. For example see Bob Lutz's blog (Vice-Chairman, General Motors Corporation) at http://fastlane.gmblogs.com

[147] Scoble, R., Israel, S, 2006, *op cit.* pp.227-232.

[148] Durodié, W., 2005, 'Risk and the Social Construction of 'Gulf War Syndrome'', *Philosophical Transactions of the Royal Society B*, 2006, 361, pp.689-695.

[149] Devji, F., 2005, *Landscapes of the Jihad*, London: Hurst & Co.

[150] Mongoven, B., 2005, 'The Evolution of Market Campaigns', *USA Today*, 27 September 2005.

[151] Gray, C.S., 2005, *op cit*, pp.55-98.

[152] Nye, J.S., Jr., 2004, *Soft Power: The Means to Success in World Politics*, Cambridge (MA): Public Affairs.

[153] Gray, C.S., 2005, *op cit*, p.95.

[154] Statement by a former UK Government official at a DEMOS seminar in 2004, supported by Senator John Cornyn, member of the US Senate Judiciary Committee and Chair of the US Senate Subcommittee on the Constitution, Civil Rights and Property Rights in: Cornyn, J., 2004, 'Ensuring the Consent of the Governed', *LBJ Journal of Public Affairs*, Fall, pp.7-10.

[155] Warren, M.E., (Ed), 1999, *op cit.*

[156] O'Neill, O., 2002, *op cit*.

[157] O'Hara, K., 2004, *op cit.*

[158] Eiser, J.R., 2004, *Public Perception of Risk*, Foresight: Office of Science and Technology, July 2004, London.

[159] O'Neill, O., 2002, *op cit*.

[160] Cornyn, J., 2004, 'Ensuring the Consent of the Governed', *LBJ Journal of Public Affairs*, Fall, p.7-10.

[161] O'Neill, O., 2002, *op cit*.

[162] Gibson, S.D., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22.

[163] Odom, W., 2003, *op cit, p.ix.* William E Odom is a former Director of the US National Security Agency.

[164] Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger.

[165] Betts, R.K., 1978, 'Analysis, War, and Decision: Why Intelligence Failures are Inevitable', *World Politics*, 31 (1) 61-89.

[166] Johnston, R., 2005, *op cit*, pp.64-66. His forecasting experts are across the board, from actuaries in insurance to analysts in intelligence.

[167] Senator Arlen Specter then became chair of the Senate Select Committee on Intelligence.

[168] _____ 1998, *The New York Times*, 4 December, 1998.

[169] US Commission on the Roles and Capabilities of the United States Intelligence Community, 1996, *Preparing for the 21st Century: An Appraisal of US Intelligence*, 1996/03/01, Washington DC: US Government Printing Office; US House Permanent Select Committee on Intelligence, 1996, *IC 21: The Intelligence Community in the 21st Century*, 1996/04/09, Washington DC: US Government Printing Office.

[170] Eisendrath, C., (Ed), 2000, *National Insecurity: US Intelligence after the Cold War*, Philadelphia: Temple University Press.

[171] Johnston, R., 2005, *op cit*, pp.xi-xii.

[172] The view is also reflected in: Zegart, A.B., 2007, "'CNN with Secrets": 9/11, the CIA, and the Organizational Roots of Failure', *International Journal of Intelligence and CounterIntelligence*, 20, 1, pp.18-49.

[173] The Oxford Intelligence Group under the guidance of intelligence scholar, Michael Herman, has done much to stimulate debate and education on matters intelligence in the UK, including preliminary engagement with the media.

[174] Ransom, H.H., 1994, 'Reflections on Forty Years of Spy-Watching', unpublished paper as cited in: Johnson, L.K., 2002, *Bombs, Bugs, Drugs, and Thugs*, New York: New York University Press, p.1.

[175] US Commission on the Roles and Capabilities of the United States Intelligence Community, 1996, *Preparing for the 21st Century: An Appraisal of US Intelligence*, 1996/03/01, Washington DC: US Government Printing Office.

[176] Best, R.A., (Ed) 2006, *Intelligence Issues for Congress*, Washington: US Congressional Research Service, p.5.

[177] Herman, M., McDonald, J.K., Masny, V., 2006, *Did Intelligence Matter in the Cold War?* Oslo: Institutt for Forsvarsstudier (Norwegian Institute for Defence Studies); Gibson, S.D., 1997, *op cit.*

[178] Goodman, M.A., 2003, *op cit.*

[179] Pringle, R.W., 2003, The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989, *International Journal of Intelligence and CounterIntelligence*, 16, pp.280-289.

[180] As noted in Chapter One (1.8), the Foreign Broadcast Information Service was subsumed into the US Director of National Intelligence's new Open Source Center in November 2005.

[181] Mercado, S., 2004, *op cit*; Pringle, R.W., 2003, *op cit.*

[182] Gibson, S.D., 1997, *op cit.*

[183] Gray, J., 2003, *Al Qaeda and What it Means to be Modern*, London: Faber & Faber.

[184] Hough, P., 2004, *Understanding Global Security*, Abingdon: Routledge, p.12.

[185] Brandt Commission, 1980, *North-South: A Programme for Survival*, The Report of the International Commission on International Development Issues, London: Pan.

[186] Shulsky, A.N., Schmitt, G.J., 2002, *op cit.*

[187] Lowenthal, M.M., 2003, *op cit.*

[188] Gray, J., 2002, *Straw Dogs: Thoughts on Humans and Other Animals*, London: Granta Books.

[189] Huntington, S.P., 2002, *The Clash of Civilizations and the Re-making of World Order*, London: Simon & Schuster; Scruton, R., 2002, *The West and the Rest: Globalization and the Terrorist Threat*, London: Continuum; Barber, B.R., 2003, *Jihad vs. McWorld: Terrorism's Challenge to Democracy*, London: Corgi Books; Buruma, I., Margalit, A., 2004, *Occidentalism: A Short History of Anti-Westernism*, London: Atlantic Books.

[190] Held, D., 2004, *Global Covenant*, London: Polity Press; Gray, J., 2003, *op cit;* Sardar, Z., Wyn-Davies, M., 2002, *op cit.*

[191] Lewis, B., 2004, *The Crisis of Islam: Holy War and Unholy Terror*, Phoenix; Gunaratna, R., 2002, *Inside Al Qae'da*, London: Hurst & Co.

[192] Greider, W., 2003, *The Soul of Capitalism: Opening Paths to a Moral Economy*, New York: Simon & Schuster; Barber, B.R., 2003, *op cit;* Cross, G.S., 2002, *An All-Consuming Century: Why Commercialism Won in Modern America*, New York: Columbia University Press.

[193] Chomsky, N., 2004, *op cit;* Buruma, I., Margalit, A., 2004, *op cit;* Pilger, J., 2002, *The New Rulers of the World*, London: Verso.

[194] O'Hara, K., 2004, *op cit.*

[195] Furedi, F., 2002, *op cit.*

[196] Gaskin, J.C.A., (Ed), 1998, *Leviathan: Thomas Hobbes*, Oxford: Oxford Paperbacks.

[197] Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger.

[198] Odom, W., 2003, *Fixing Intelligence for a More Secure America*, New Haven: Yale.

[199] Eisendrath, C., (Ed), 2000, *op cit.*

[200] US Senate Confirmation Hearing; James Woolsey, 3 February 1993. Reported in: *The Guardian*, 4 February 1993.

[201] Clift, A.D., 2003, 'From Semaphore to Predator: Intelligence in the Internet Era', *Studies in Intelligence*, 47, 3, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no3/article06.html

[202] Berkowitz, B.D., Goodman, A.E., 2000, *op cit.*

[203] A 'source' cited in Johnson, L.K., 2003, Preface to a Theory of Strategic Intelligence, *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[204] Thompson, B.G., 2006, *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*, US House Committee on Homeland Security Democratic Staff, Washington, DC.

[205] US Senate Committee on Governmental Affairs, 2004, *Summary of Intelligence Reform and Terrorism Prevention Act of 2004*, US Senate, 2004/12/06, available at: http://intelligence.senate.gov/iraqreport2.pdf

[206] US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company, available at: http://www.9-11commission.gov/report/911Report.pdf; Silberman, L.H., Robb, Charles S., 2005, *US Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC., Report No: 20503, March 2005, available at: http://www.wmd.gov/report/report.html

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

[208] Efraim Halevy is a former Head of the MOSSAD, Israel's foreign intelligence service.

[209] Halevy, E., 2004, *Intelligence and the Making of Foreign Policy: A Personal Reflection*, 21 June 2004.

[210] Kissenger, H., 1994, *Diplomacy*, London: Simon & Schuster.

[211] Treverton, G.F., 2003, 'Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons', *Intelligence and National Security*, 18, 4, pp.121-140.

[212] *Ibid.*

[213] Betts, R.K., Mahnken, T.G., 2003, (Eds). *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, Portland: Frank Cass, pp.60-62.

[214] Shulsky, A.N., Schmitt, G.J., 2002, *op cit.*

[215] *Ibid, p.156.*

[216] Hulnick, A.S., 1999, 'Openness: Being Public About Secret Intelligence', *International Journal of Intelligence and CounterIntelligence*, 12, 4, pp.463-483.

[217] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press; Odom, W., 2003, *Fixing Intelligence for a More Secure America*, New Haven: Yale; Lowenthal, M.M., 2003, *op cit;* Markowitz, J., 2003, 'Open Source: In Support of All-Source Intelligence', *Open Source Solutions*, Washington DC, USA; Johnson, L.K., 2002, *Bombs, Bugs, Drugs, and Thugs*, New York: New York University Press; Steele, R.D., 2002, *Information Peacekeeping & the Future of Intelligence*, 18th November 2002 (unpublished manuscript); Steele, R.D., 2002, *The New Craft of Intelligence Personal, Public, & Political*, Oakton, Virginia: OSS International Press; Steele, R.D., 2001, *op cit*, R.D., 2000, Possible Presidential Intelligence Initiatives, *International Journal of Intelligence and CounterIntelligence*, 13, 4, pp.409-423; Berkowitz, B.D., Goodman, A.E., 2000, *op cit*; Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger; Holden-Rhodes, J.F., 1997, *Sharing the Secrets: Open Source Intelligence and the War on Drugs*, West Port, CT: Praeger.

[218] *Intelligence and National Security Journal*, Volume 18, Issue 4, 2003.

[219] Goodman, M.A., 2003, *op cit.*

[220] Gibson, S.D., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22.

[221] Furedi, F., 2004, *Where Have all the Intellectuals Gone? Confronting 21st Century Philistinism*, London: Continuum; Giddens, A., 2002, *op cit;* Angell, I., 2000, *op cit;* Rees, M., 2003, *op cit;* Rischard, J.F., 2002, *op cit.*

[222] Wark, W.K., 2003, Learning to Live With Intelligence, *Intelligence and National Security*, 18, 4, pp.1-14; Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[223] De Jong, B., Platje, W., Steele, R.D., (Eds), 2003, *op cit.*

[224] Joseph Hayes cited in Johnston, R., 2005, *op cit*, p.160.

[225] *Ibid*.

[226] *Ibid*.

[227] Steele, R.D., 2002, *The New Craft of Intelligence Personal, Public, & Political*, Oakton, Virginia: OSS International Press.

[228] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*; Wark, W.K., 2003, 'Learning to Live With Intelligence', *Intelligence and National Security*, 18, 4, pp.1-14.

[229] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663; Gibson, S.D., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22.

[230] Lowenthal, M.M., 2003, *op cit.*

[231] The EU, although not globally representative is a global player. There is some effort within the EU to 'harmonise' intelligence and security across the presently 25 member states although meaningful outcomes will be the arbiter of effectiveness. See: Muller-Wille, B., 2004, *'For Our Eyes Only? Shaping an Intelligence Community Within the EU'*, Occasional Paper No. 50 January 2004 pp.1-51, available at: http://www.iss-eu.org/occasion/occ50.pdf (19 August 2004)

[232] Christensen, C., 2003, *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*, Boston: Harvard Business School Press.

[233] Giddens, A., 2002, *op cit.*

[234] Pringle, R.W., 2003, *op cit;* Hulnick, A.S., 2002, 'The Downside of Open Source Intelligence', *International Journal of Intelligence and CounterIntelligence*, 15, 4, pp.565-579.

[235] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[236] Hulnick, A.S., 2004, *op cit*, p.65.

[237] Friedman, G., 2004, *America's Secret War: Inside the Hidden Worldwide Struggle Between the United States and its Enemies*, London: Doubleday, Random House, p. 250-251.

[238] Pidgeon, N., Kasperson, R., Slovic, P., (Eds), 2003, *The Social Amplification of Risk*, Cambridge: Cambridge University Press.

[239] See for example following the Battle of Trafalgar: 'Foreign Intelligence from the Dutch Papers; the French Papers; and the Hamburgh *(sic)* Papers', 7 November 1805, *The Times*, No. 6572, p.2.

[240] Friedman, R.S., 1998, *op cit.*

[241] Smith, M., 2003, *The Spying Game: The Secret History of British Espionage*, London: Politico's Publishing.

[242] *Ibid.*

[243] Mercado, S., 2004, *op cit.*

[244] Reuser, A., 2006, 'Sharing Information from a Dutch Perspective', presentation to Dutch Ministry of Defence, Defence Intelligence and Security Service, June 2006, available at: http://www.google.com/custom?hl=en&lr=&cof=&domains=oss.net&q=reuser&btnG=Search&sitesearch=oss.net

[245] Taleb, N.N., 2004, *op cit*; Taleb, N.N., 2007, *op cit.*

[246] Harvard Business School, (Ed), 1998, *Harvard Business Review on Knowledge Management*, Boston: Harvard Business School Publishing.

[247] Johnson, L., 2003, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, 22, 1, pp.1-28.

[248] Lowenthal, M.M., 2003, *op cit.*

[249] Davenport, T.H., Prusak, L., 2000, *Working Knowledge: How Organizations Manage What They Know*, Boston: Harvard Business School Press.

[250] Wheaton, K.J., 2001, *The Warning Solution: Intelligent Analysis in the Age of Information Overload*, Fairfax: AFCEA International Press (AIP).

[251] Lowenthal, M.M., 1999, 'Open Source Intelligence: New Myths, New Realities', *Intelligencer*, 10,1, pp.7-9, available at: http://www.oss.net/dynamaster/file_archive/040319/ca06aacb07e5cb9f25f21babf7ef2bf0/OSS1999-P1-08.pdf

[252] *Ibid.*

[253] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press, p.119.

[254] *Ibid*, pp.119-120. This creates practical juxtaposition for the intelligence function with Infosphere's argument that OSINT cannot be satisfactorily conducted inside a closed environment.

[255] US Department of Defense, 2004, *Dictionary of Military and Associated Terms:* JP 1-02, p.384.

[256] The US military experience of OSINT generated between its practitioners and traditional closed intelligence agencies has been fractious. This is apparent throughout Steele's writing; but also observed by author's conversations with the two OSINT organisations – VIC/APAN and USSOCOM.

[257] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[258] *Ibid*, p.113.

[259] UK Intelligence and Security Committee, 2004, *Annual Report 2003-2004*, Report No: Cm 6240, 2004/06/29, p. 5.

[260] Sir David Omand at Gresham House 2005, available at: http://gresham.ac.uk/events.asp?pageid=4&frmProfessor=118&frmKeyword=Keyword&frmAllDates=on&image.x=6&image.y=17

[261] The Internet is divided into the surface web (aka superficial web) and deep web (aka invisible web). The deep web comprises those sites that are on the Internet but inaccessible to conventional search engines (e.g. Google). There are several web sites dedicated to searching the deep web. The most comprehensive of these is Direct Search maintained by Gary Price, a reference librarian at George Washington University (http://freepint.com/gary/direct.htm). Equally, there are an increasing number of search tools becoming commercially available for deep-web search such as Cogenta. The deep web contains approximately 7,500 terabytes of information (550 billion documents), compared to 19 terabytes (1 billion documents) on the surface web (a Terabyte is 1,000 Gigabytes). If the Internet is growing at

approximately a million documents a day and your sole recourse to gathering information is Google then the implication for information collection and collation is ominous.

[262] Smith, A., 2005, *Making Books Easier to Find*, available at: http://googleblog.blogspot.com/2005/08/making-books-easier-to-find.html

[263] CIA, 2001, *Are You Ready? Implications of a Changing Global Environment for Open Source Intelligence*, Washington: Global Futures Partnership in the Directorate of Intelligence, dated 1 July 2007.

[264] SACLANT Intelligence Branch, 2002, *Intelligence Exploitation of the Internet*, October 2002, pp.1-103.

[265] US Department of Defense Joint Chiefs of Staff, 2004, *Joint and National Intelligence Support to Military Operations*, JP 2-01.

[266] Bokhari, K., 2005, *The World Wide Web of Jihadists*, 4 December 2005, available at: http://www.stratfor.com

[267] Hulnick, A.S., 2004, *op cit*, p.51.

[268] Dehqanzada, Y., Florini, A., 2000, 'Secrets for Sale: How Commercial Satellite Imagery will Change the World', in: SACLANT Intelligence Branch, 2002, *NATO Open Source Intelligence Reader*.

[269] Available at: http://www.cartographic.com/xq/ASP/AreaID.33/RegionID.131/CategoryID.5/ProductID.2308/middle_east/iran/qx/topographic_maps.asp as at September 2003

[270] Steele, R.D., 2001, *op cit.*

[271] See: http://www.oss.net

[272] Baird, Z., Barksdale, J., 2003, *Creating a Trusted Network for Homeland Security*, Markle Foundation Task Force on National Security in the Information Age, Report No: 2, New York. See Appendix H for a complete list at: http://www.markle.org/downloadable_assets/nstf_report2_full_report.pdf (9 January 2006).

[273] The Surveillance Studies Network, (Ed) 2006, *A Report on the Surveillance Society*, London: The Information Commissioner, September 2006, available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf

[274] SACLANT Intelligence Branch, 2001, *NATO Open Source Intelligence Handbook*, November 2001, pp.1-49; SACLANT Intelligence Branch, 2002, *NATO Open Source Intelligence Reader*, February 2002, pp.1-109.

[275] Steele, R.D., 1996, 'Creating a Smart Nation: Strategy, Policy, Intelligence, and Information', *Government Information Quarterly*, 13, 2, pp.159-173.

[276] *Anonymizer* sales quarterly report clipping, available at: http://www.anonymizer.com/consumer/media/press_releases/08292005.html

[277] Eisendrath, C., (Ed), 2000, *op cit.*

[278] US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company.

[279] US Senate Committee on Governmental Affairs, 2004, *Summary of Intelligence Reform and Terrorism Prevention Act of 2004*, US Senate, 2004/12/06.

[280] Perry-Barlow, J., 2002, 'Why Spy?', *Forbes*, 10th July, 2002.

[281] Hulnick, A.S., 2004, *op cit*, p.65-66; Hulnick, A.S., 2002, *op cit.*

[282] UK Privy Councellors, 2004, *Review of Intelligence on Weapons of Mass Destruction* (The Butler Review), House of Commons, Report No: HC 898.

[283] Pidgeon, N., Kasperson, R., Slovic, P., (Eds), 2003, *op cit;* see also: 'Spiked online' available at: http://www.spiked-online.com/ for a political journalistic effort to establish credible, meaningful reporting and a call for informed debate on substantive issues of the day.

[284] Trim, P.R., 2000, 'The Company Intelligence Interface and National Security', *International Journal of Intelligence and CounterIntelligence*, 13, 2, pp.204-214.

[285] Newman, V., 2002, *The Knowledge Activist's Handbook*, Oxford: Capstone.

[286] Control Risks Group, Hazard Management Solutions, Kroll, Risk Advisory Group to name a few.

[287] Terrorism at Saint Andrews University, the Resilience Centre at Cranfield University, Kidnap at the Foreign Policy Research Centre and Geo-political risk at the Economist Intelligence Unit to name a few.

[288] Nye, J.S., Jr., 2004, *op cit.*

[289] Hood, C., 2006, Transparency in Historical Perspective', in Hood, C., Heald, D., 2006, *Transparency: The Key to Better Governance?*, Oxford: Oxford University Press, pp.3-23.

[290] Steele, R.D., 1996, 'Creating a Smart Nation: Strategy, Policy, Intelligence, and Information', *Government Information Quarterly*, 13, 2, pp.159-173.

[291] Johnston, R., 2005, *op cit*, pp.24-25.

[292] Face validity is the notion that an instrument measures what it is intended to measure without the need for supporting material.

[293] Cavendish, A., 1997, *Inside Intelligence*, London: HarperCollins.

[294] Sandman, P.M., 1989, 'Hazard Versus Outrage in the Public Perception of Risk', in: Covello, V., McCallum, D., Pavovla, M., (Eds), 1989, *Effective Risk Communication: The Role and Responsibility of Government and Non-Government Organizations*, New York: Plenum Press, pp.45-49.

[295] Steele, R.D., 2001, *op cit.*

[296] De Jong, B., Platje, W., Steele, R.D., (Eds), 2003, *op cit.*

[297] SACLANT Intelligence Branch, 2002, *NATO Open Source Intelligence Reader*, February 2002, pp.1-109.

[298] Cited in: Steele, R.D., 2001, *op cit*, p.62.

[299] Jaeger, C.C., Renn, O., Rosa, E.A., Webler, T., 2001, Risk, Uncertainty, and Rational Action, London: Earthscan.

[300] Durodie, W., (Ed) 2005, *The Domestic Management of Terrorist Attacks*, London: Report No: L147251003.

[301] Hyams, K.C., Murphy, F.M., Wessely, S., 2002, '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*, 27, 2, pp.273-291.

[302] Bennett P., Coles D., McDonald A., 1999, 'Risk Communication as a Decision Process', in: Bennett P., Calman K., (Eds), *Risk Communication and Public Health*, Oxford: Oxford University Press, pp.207-221.

[303] US Senate Committee on Armed Services, Hearings on the National Defense Establishment, 1st Session, 1947, pp 525-28, as recounted in Grose, P., 1994, *Gentleman Spy: The Life of Allen Dulles*, p. 275. New York.

[304] Conversation with Markowitz, *op cit*.

[305] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[306] NATO, EUROPOL, EU, UK MOD, Swedish MOD, Dutch MOD, US DIA, CIA, UK HMRC-LE to list a few in the public sector.

[307] Elcock (Canadian Intelligence and Security Service), Oehler (US Intelligence Community Nonproliferation Center) and Scalingi (Los Alamos National Laboratory), as cited in: SACLANT Intelligence Branch, 2002, *NATO Open Source Intelligence Reader*, p.73.

[308] Hulnick, A.S., 2004, *op cit*, p.6.

[309] The EUROPOL case-study (Interview EUROPOL 4) describes anecdotal evidence of OSINT as proportion of final intelligence. See Appendices.

[310] Michael Scheuer quoted in: Glasser, S.B., 2005, 'Probing Galaxies of Data for Nuggets', *Washington Post*, 25 November 2005, available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/11/24/AR2005112400848.html

[311] Steele's PIB estimate at http://www.oss.net and Private correspondence, Steele - Gibson, 3 October 2003.

[312] US Commission on the Roles and Capabilities of the United States Intelligence Community, 1996, *Preparing for the 21st Century: An Appraisal of US Intelligence* (Brown-Aspin Commission), Washington DC: US Government Printing Office.

[313] Nolte, W., 2005, *The New Look in American Intelligence Training*, presentation to the Oxford Intelligence Group, St Anthony's College, Oxford, 5 December 2005. William Nolte was appointed Deputy Assistant Director of Central Intelligence for Analysis and Production in 2004 commensurate with the creation of the office of DNI.

[314] Of course with Moynihan he was preaching to the converted. Moynihan has described the CIA as stupid and called for its abolition over the years. Washington Post 24 July 1994, p. C-3.

[315] Kennan, G.F., 1997, *The New York Times*, 18 May 1997, p.E-17.

[316] Conversation with Dr Joe Markowitz (October 2003), former Director of the US government's (CIA) Community Open Source Programme.

[317] *Ibid.*

[318] Mercado, S., 2004, *op cit.*

[319] US Army, 2004, *US Army Field Manual - Intelligence* 2-0, p.I-8.

[320] US Department of Defense Joint Chiefs of Staff, 2004, *Joint and National Intelligence Support to Military Operations JP 2-01*, pp.III,56-57.

[321] UK HM Treasury, 2004, *2004 Spending Review: Public Service Agreements 2005-2008*, HM Treasury, Report No: Cm 6238, 2004/07/12.

[322] Wilson, E.O., 2003, *The Future of Life*, London: Abacus.

[323] *Ibid*.

[324] *Ibid.*

[325] Odom, W., 2003, *Fixing Intelligence for a More Secure America*, New Haven: Yale, p.32.

[326] Strictly-speaking, the Single Intelligence Account (SIA) refers to the combined budgets of the British Security Service, the UK's Secret Intelligence Service and the UK's Government Communications Headquarters (GCHQ). Their individual allocations are not disclosed for security reasons. Additionally, the term SIA also represents a useful collective description for the three principle UK intelligence and security agencies.

[327] http://www.fas.org

[328] Hillson, D., Murray-Webster, R., 2005, *Understanding and Managing Risk Attitude*, Aldershot: Gower Publishing.

[329] Tussing, B.B., 2003, *op cit*, p.22.

[330] Silberman, L.H., Robb, Charles S., 2005, *US Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC., Report No: 20503, March 2005, available at: http://www.wmd.gov/report/report.html p.378.

[331] Lahnemann, W.J., 2003, Outsourcing the IC's Stovepipes, *International Journal of Intelligence and CounterIntelligence*, 16, pp.573-593.

[332] *Ibid*.

[333] US House of Representatives/Senate, 108th Congress 2nd Session, Conference Report 108, dated 7 December 2004, O:\ARM\ARM04J46.LC, available at: http://www.fas.org/irp/congress/2004_rpt/h108-796.pdf (9 December 2004).

[334] Transparency International, 2003, *Global Corruption Report 2003: Access to Information*, London: Profile Books.

[335] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press, p.119.

[336] Speaker at Open Source Solutions Conference, Washington, November 2004.

[337] Steele, R D., 2005, Memorandum for the Record on OSINT within USG, DoD and USA, dated 5 January 2005, available at http://www.oss.net

[338] UK Privy Councellors, 2004, Review of Intelligence on Weapons of Mass Destruction (The Butler Review), House of Commons, Report No: HC 898, 2004/07/14.

[339] Lowenthal, M.M., 2003, *op cit.*

[340] Klinke, A., Renn, O., 2002, *op cit.*

[341] Eiser, J.R., 2004, *op cit.*

[342] Tussing, B.B., 2003, *op cit.*

[343] Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger.

[344] I am grateful to Professor Loch Johnson (Georgia University) for the reference to OSINT as a matrix.

[345] Dupont, A., 2003, *op cit.* I am also grateful to Chris Donnelly who expressed a similar concept to the author in his analogy with yeast and dough in bread. Dough is open source and yeast is the 'extra' ingredient that makes it 'rise'. The morale of the analogy is more direct – you cannot make leavened bread without either of them.

[346] I am grateful to Mats Bjore, who identified the idea of OSINT having to work outside the environs of closed intelligence.

[347] Mercado, S., 2004, *op cit.*

[348] The idea of an independent UK national OSINT agency (discussed later) has been received with interest by the few parties that I have discussed the idea with.

[349] Interestingly, the US Special Operations Command now leads the way in pioneering the application of OSINT, albeit virtually on its own.

[350] Berkowitz, B.D., Goodman, A.E., 2000, *op cit.*

[351] Chris Donnelly was then the Director of the Soviet Studies Research Centre, now known as the Conflict Studies Research Centre.

[352] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[353] Lowenthal, M.M., 1999, *op cit.*

[354] Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[355] O'Neill, O., 2002, *op cit.*

[356] Private conversation with open source practitioners.

[357] O'Neill, O., 2002, *op cit.*

[358] Bean, H., 2007, *op cit.*

[359] *Ibid.*

[360] Douglas Naquin quoted in: Glasser, S.B., 2005, 'Probing Galaxies of Data for Nuggets', *Washington Post*, 25 November 2005, p.A35, available at: http://www.washingtonpost.com/wp-dyn/content/article/2005/11/24/AR2005112400848.html

[361] Bean, H., 2007, *op cit.*

[362] *Ibid*,p.253.

[363] Croom, H.L., 1969, *op cit.*

[364] Mercado, S.C., 2005, 'Reexamining the Distinction Between Open Information and Secrets', *Studies in Intelligence: Journal of the American Intelligence Professional*, 49, 2, available at: https://www.cia.gov/csi/studies/Vol49no2/reexamining_the_distinction_3.htm .

[365] *Ibid*.

[366] Sims, J. E., Gerber, B., (Eds), 2005, *Transforming US Intelligence*, Washington, DC.: Georgetown University Press, pp.63-78.

[367] The 1996 Aspin-Brown commission challenged Steele and the CIA to provide a background brief on Burundi within a set time period. The results showed some significant advantages in Steele's open source route.

[368] Loch Johnson subsequently questioned this particular 'experiment', suggesting that the underlying assumptions and rules for its conduct were somewhat unfair to the intelligence community.

[369] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*, p.8.

[370] The DNI's 100-Day Plan for Integration and Collaboration rather suggests that such endeavours have to be forced. See: ODNI US IC 100 Day Plan for INTEGRATION and COLLABORATION *(sic)* issued on 11 April 2007, available at: http://www.dni.gov/100-day-plan/100-day-plan.pdf

[371] Johnston, R., 2005, *op cit*, pp.xiii-xx.

CHAPTER THREE

RESEARCH METHODOLOGY

> "If the research is worth doing, then one is likely to be dealing with a problem, which is not fully understood, and for which the ideal course of investigation cannot be charted in advance."
>
> Easterby-Smith, Thorpe & Lowe, 2002.[1]

3.0 Introduction

Chapter Two has demonstrated that, within the intelligence community, OSINT is widely perceived as punching beyond its weight in comparison to the traditional closed sources. What is unclear is how OSINT specifically contributes to the conduct of the intelligence function. The literature begins to isolate some descriptors of contribution, but they are neither consistent nor comprehensive. Thus, a research gap exists, which this research work occupies. Specifically, it addresses the hypothesis set out in the research question: that open source exploitation contributes to intelligence in a way that can be described by key high order factors. This chapter derives an optimum research strategy in order to link data collection with that research question, and answer it.

The chapter is in two parts. First, an overview of research methodology is discussed in order to determine an optimum balance between the philosophical worldview of the researcher and the needs of the research topic. The researcher's philosophical position is clearly established as interpretivist or phenomenological rather than positivist. 'Case-study' is defended as the best strategy for exploring the phenomenon of open source exploitation. Second, the research strategy and design for this study are chosen. The design includes: the choice of study cases (units of analysis); the use of semi-structured interview method; identification of the informants from whom data will be collected; the variables to be observed; the research programme; and the limitations or weaknesses of the research.

3.1 Part One: Research methodology overview

> "It is a capital mistake to theorise before one has data."
>
> Arthur Conan Doyle. [2]

3.1.1 Research - purpose, process, logic, outcome

Collis and Hussey suggest that the conduct of research from inception to conclusion is determined by its purpose, process, logic and outcome.[3] Yin includes the same determinants within his definition of the 'strategy' of research.[4] These four entities form four key questions that have exercised the research debate for many years:

- Is the research purpose (or aim) exploratory, descriptive, explanatory or predictive in nature?
- Is it essentially quantitative or qualitative in process?
- Is the research logic deductive or inductive? That is to say, respectively, does the research test a particular hypothesis against many examples or does it formulate theory from observation of many data?
- Is the research applied or pure?[5] That is to say, respectively, does the research solve a problem or contribute to understanding? Collis and Hussey argue that the latter is more pertinent to knowledge contribution.[6]

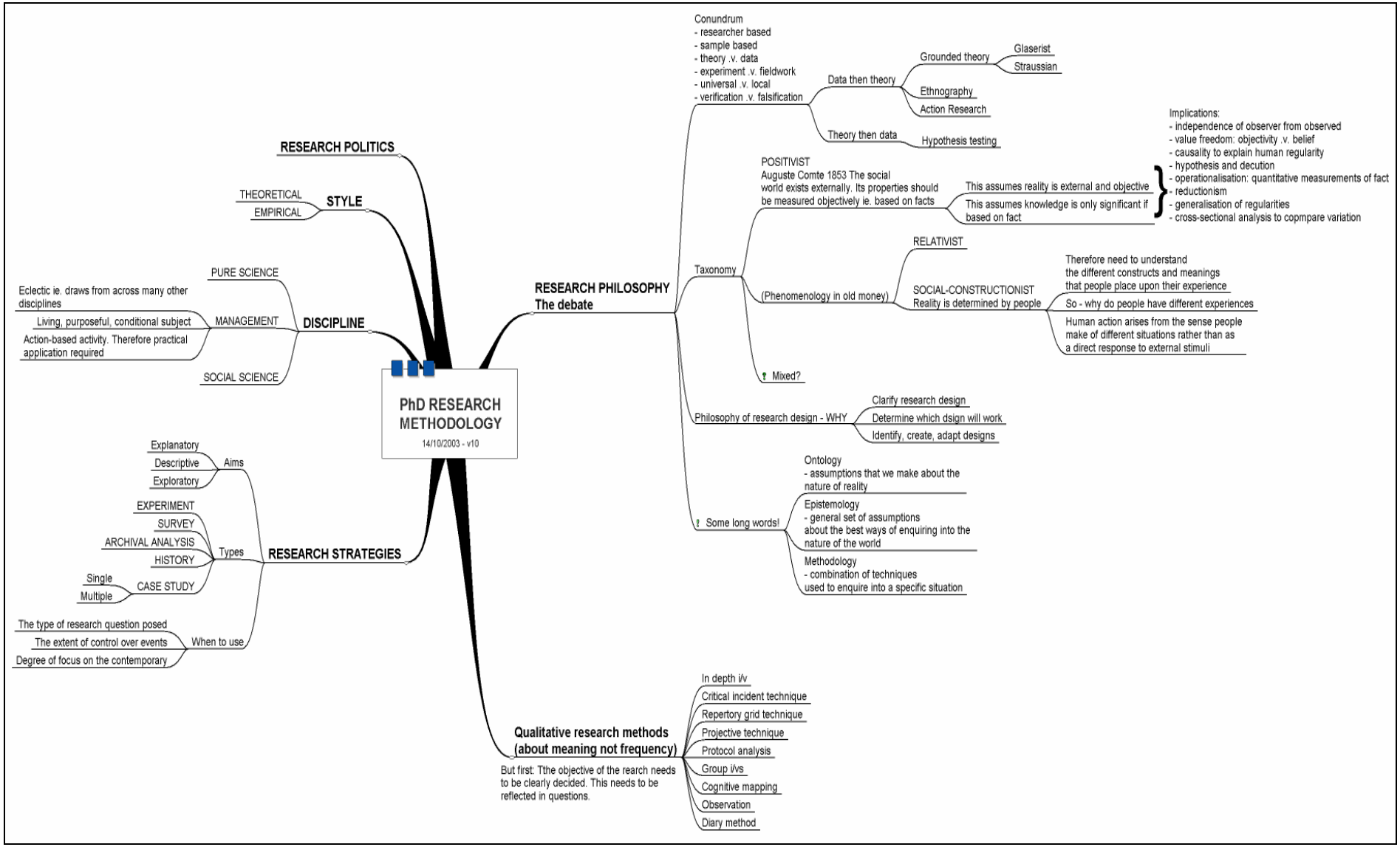
These questions are influenced and underpinned by the evolving and often competing paradigms of research philosophy. Of these the quantitative versus qualitative debate is the most philosophically contentious. Fortunately, the philosophical debate that underpins each question is resolvable. Easterby-Smith, Thorpe and Lowe suggest that movement from theoretical research discussion to practical research action is possible on two counts:[7]

- First, any research methodology and therefore ultimately research design, rather than being polarised or strictly categorised, can be derived across a spectrum of choice. Thus, research methods are employed according to their appropriateness to the study being undertaken, rather than their ability to resolve philosophical debate.

- Second, research methodology, evidenced by choice of research strategy and rationale of research design, is also influenced by the researcher's own ontological and epistemological position. That is to say a researcher's own worldview and the researcher's belief as to how knowledge is created moves research from debate to action.

Thus, any debate, which rages around the choice of methodology, is ultimately resolved by a combination of the needs of the study and the views of the investigator. Therefore, it becomes important to establish the researcher's philosophical paradigm and the study's philosophical needs before a methodology can be chosen. Figure 3.1 below illustrates this author's overview of research methodology.

Figure 3.1: Overview of research methodology



Source: Author

3.1.2 Research philosophy

Easterby-Smith *et al* assert that: "Failure to think through philosophical issues … can seriously affect the quality of (management) research."[8] They further contend that: "…philosophical factors affect the overall arrangements, which enable satisfactory outcomes from the research activity"[9]

It is interesting to note that the last half-century has seen something of a transformation, or at least an extension, of the philosophical paradigms underpinning research methodology.[10] Compte's 18th century positivist approach has given ground to what Habermas describes as interpretivist, Collis and Hussey describe as phenomenological and Easterby-Smith *et al* describe as social-constructionist.[11] Smith relates it to the quantitative versus qualitative debate by arguing that: "In quantitative research, facts act to constrain our beliefs; while in interpretive research beliefs determine what should count as facts".[12] This reflects an increasing awareness that the act of measurement, however objective and detached from the object of measurement, changes the object being measured.[13] Heisenberg's Uncertainty Principle (or as it later became more descriptively known – Indeterminacy Principle) of 1927 summarises the position: "The more precisely the position is determined, the less precisely the momentum is known in this instant, and vice versa."[14] Easterby-Smith *et al* interpret the conundrum to mean: "It is never possible to obtain full and objective information about the observed state of the phenomenon being discovered".[15]

Research philosophy clarifies the research debate somewhat by embarking upon classification of the various arguments into taxonomy. Easterby-Smith *et al* posit a classification separating out research into positivist, relativist and social-constructionist philosophical traditions.[16] Cavaye suggests something similar to Easterby-Smith *et al*'s 1991 classification, when he polarises research philosophy as positivist or interpretive.[17] Interestingly, and supporting the view above that the locus of research methodology is on the move, this represents a modification of their earlier work in which they differentiated only two philosophies; positivism and phenomenology.[18] The movement

of three authors over eleven years bears testimony to Heisenberg's exposition of the significance of the impact of observation on the observed.

So, it seems then that the reality of research is to be found somewhere on a continuum between two extremes. However, most writers on the subject acknowledge that research philosophy transgresses such rigid prescription in practice. Indeed, rather, than being so easily polarised, they are actually somewhat artificial, vague, unclear and merging. For example, Morgan and Smircich articulate movement along this continuum from positivist to phenomenological in 6 stages:[19]

> "Positivist
>
> 
>
> - Reality as a concrete structure
> - Reality as a concrete process
> - Reality as a contextual field of information
> - Reality as a realm of symbolic discourse
> - Reality as a social construction
> - Reality as a projection of human imagination
>
> Phenomenological"

By extension, the research philosophy that one tends towards will ultimately reflect one's own worldview. Essentially, such a worldview must address the question of whether reality is to be considered an external, objective phenomenon that can be measured, or an internal, social construct, which cannot be measured because it is integral to the construct. Then one must determine, at least, where one sits along that continuum. If the theoretical physics of Heisenberg and the brief examination of risk theory in Chapter Two (2.2.2) are anything to go by, then this author is persuaded that research philosophy and hence methodology is influenced by 'a bit of both'. Either way (and it is very unlikely to be either way - rather a mix of ways somewhere along the spectrum) one's broad alignment to positivist or phenomenological ends of the research philosophy spectrum will predispose one to a research strategy.

Collis and Hussey describe the pure positivist approach as: "(It is) based upon the assumption that social reality is independent of us and exists regardless of whether we are aware of it".[20] In this case, ontology and epistemology can be separated since: "The act of investigating reality has no effect on that reality".[21] Conversely, the phenomenological approach is predicated on the assumption that all behaviour is generated from within the human mind or constructed. Here, it is difficult to separate the ontological from the epistemological. Furthermore, as Collis and Hussey suggest: "This qualitative approach stresses the subjective aspects of human activity by focusing on the meaning, rather than the measurement, of social phenomena".[22] Van Maanen echoes this theme when he argues that phenomenological, interpretive, qualitative techniques are about meaning not frequency.[23]

Finally for philosophy, one must consider whether one's approach is going to reduce the subject to such a meaningless set of variables and observations that the result loses all touch with the original subject. Ormerod argues very persuasively that traditional economic theory and its attendant models - one of the social sciences heavily influenced by positivism - has become the epitome of reductionism in its most dangerous form.[24] The process of reducing a sophisticated entity changes the nature of the phenomenon being examined without necessarily revealing insight into the object of study. It remains a paradox of systems involving human agency that we think we can predict, plan and control them based upon knowledge of the behaviour of its working parts. At aggregate levels, systems, despite the purposeful and intentional behaviour of their component parts, display random behaviour due to the infinite number of interactions the parts have with each other.[25] This is not to say that in order to understand entities better abstraction from detail to simplicity is not without merit; but it should not be without caution also. It can be stated confidently at this juncture that the subject of this thesis is sympathetic to insight and understanding, and wary of reductionism.

3.1.3 Research methodology

Research methodology is the process whereby a researcher, taking into account the philosophical paradigms of research, arrives at a research design that is most suitable

and applicable to the research aim. It represents the critical fulcrum of the entire research study process.[26] Methodology is the encompassing boundary of research that has research design as its focus and centre. Methodologies have become associated with the main philosophical paradigms that underpin them. Table 3.1 categorises this relative association:

Table 3.1: Methodologies and their associated philosophical paradigms

POSITIVISTIC	**PHENOMENOLOGICAL**
Cross-sectional studies	Action research
Experiment	Case-studies
Longitudinal studies	Ethnography
Surveys	Feminist
	Grounded theory
	Hermeneutics
	Participative enquiry

Source: Adapted from Collis and Hussey, 2003.[27]

Van Maanen probably expresses it best when he suggests that the qualitative method, of which case-study is a leading light, is at best an "umbrella term" of interpretive techniques seeking to explore the meaning not frequency of socially occurring phenomenon.[28] He adds that qualitative studies are conducted: "*in vivo*, close to the point of origin" and do not prohibit: "the logic of scientific empiricism" or the rigorous scientific method. Indeed, qualitative and quantitative methods are not in competition or mutually exclusive; but can be integrated and mutually supportive.[29]

It seems then that methodology has two functions: an overarching research approach spanning philosophical paradigm to data collection methods, as well as being the practical vehicle that moves research from thought to action. In this latter regard it also seems to possess equivalence with the term 'strategy'. The literature on research frustratingly interchanges the terms 'strategy' and 'methodology'. Methodology is perhaps more akin to philosophical paradigm and thus more ontologically oriented, whereas strategy is more akin to research design and thus more epistemologically

oriented. However, if seen as the lynchpin between thinking and doing, the two terms can mutually co-exist. As far as is possible, methodology is used in this thesis to characterise the whole approach to research, while strategy is used to characterise the route to research design.

3.1.4 Research strategy and design

Yin defines research strategy as providing the transition mechanism between research philosophy and phenomenon of research.[30] It is the first practical step away from the theory of research and towards the design of research. He identifies five research strategy options for social science research: experiment; survey; archival analysis; historical; and case-study. He then poses three fundamental conditions to consider for each strategy, expanded in Table 3.2 below, when choosing one over any other:[31]

- "The type of research question posed.
- The extent of control an investigator has over actual behavioural events.
- The degree of focus on contemporary as opposed to historical events."

Table 3.2: Research strategy choice

CONDITION / STRATEGY	Form of research question	Requires control of behavioural events?	Focuses on contemporary events
Experiment	How, why?	Yes	Yes
Survey	Who, what, where how many how much?	No	Yes
Archival analysis	Who, what, where how many how much?	No	Yes/No
History	How, why?	No	No
Case-study	How, why?	No	Yes

Source: Yin, 2003.[32]

Again, the literature on research is not always consensual. Yin's approach seems slightly at odds with Easterby-Smith *et al* who acknowledge the different strategies but equate them with data collection methods rather than strategy.[33] Collis and Hussey acknowledge the alternative strategies, but prefer to call them methodologies, and then relate them to the philosophical paradigm poles rather than the epistemological taxonomy that Yin does.[34]

Yin's strategies are not hierarchical but designed to best fit the circumstances of the research study. The taxonomy is not discrete or sharp but overlapping. The aim is to make the best strategy-fit for the research and thus design, where design is the focal point of research methodology. In other words, research design is the logic that links the data to be collected from the research study with the initial research aim and objectives, and all of these with the conclusions drawn. Thus, research design demonstrates a logical chain of evidence stretching from the research problem through data collection to conclusions. It is the plan for implementing the chosen research strategy.

3.1.5 Case-study

Case-study is a qualitative research method used for the collection and analysis of empirical data. McCutcheon and Meredith, justifying the case-study method to the normally quantitatively and positivist oriented discipline of operations management, conclude as one of its benefits: "(However), if done properly, case-study research can provide discoveries not possible through other methods".[35] Case-study is a research method now routinely utilised in management disciplines, increasingly utilised in many social sciences, and gaining popularity in most disciplines.[36]

There is very little research methodology literature concerned with case-study that does not at some stage reference the span of Yin's work conducted between 1981 and 2003. Indeed Easterby-Smith *et al* themselves acknowledge that: "Robert Yin is probably the best known exponent of this approach".[37] The third edition of his book, "Case-study Research: Design and Methods", has been re-printed thirty-seven times. Yin's

essential contributions include; the provision of a typology of case-study design, the essential requirement of case-study validity and reliability, and the logic of case-study replication and data triangulation.

There are other contributors to the research methodology and case-study debates beyond Yin. Miles and Huberman have contributed analytical techniques for qualitative data, including tables and graphs to preserve the intrinsic value of the data that might otherwise have been lost by quantitative methods.[38] Glaser and Strauss, early collaborators in pioneering grounded theory, advanced the idea that theory can emerge from a continuous comparison of data.[39] However, they have since 'fallen out' and gone their separate ways to develop offshoots of grounded theory known as 'Glaserian' and 'Straussian'. The former advocates an open almost serendipitous approach to research; the latter a more prescribed and structured approach.

Eisenhardt adopts the principals of grounded theory to expand the argument for case-study methodology as being a valid method for inductive theory building.[40] She develops a logical strategy and framework to effect a highly iterative process of data collection and analysis. While the results of such theory building strategy should be: "novel, testable and empirically valid" it should also deliver 'insight' as the test of good research. For Eisenhardt, the significance of the research question is as a tool to focus data collection rather than testing a hypothesis. She states that: "Theory-building research is begun as close as possible to the ideal of no theory under consideration and no hypothesis to test".[41] Rather than having an initial question, she advocates defining a research problem, some relevant variables, and then avoid thinking about any relationships between these variables until data collection and analysis suggests it.

While some research theoreticians advocate a deductive approach (hypothesis testing) and others an inductive approach (theory generation) they both recommend case-study as the medium. Yin is more closely aligned with case-study research leading from theory to data, Eisenhardt the reverse; but both place strong emphasis on the need for a good research question to affect either. Yin's is a more structured approach, leaving less to chance than Eisenhardt, who even acknowledges the part that serendipity can

play in theory building, but is no less rigorous in the scientific iterative method that she advocates.

Bonoma summarises the critical conundrum of these two paths to knowledge; the deductive, almost purely theoretical approach, versus the inductive, characterised by a qualitative, clinical approach.[42] He advocates case-study methodology, as a route to contextual richness and external validity or generalisability, whereby phenomena can best be understood when examined in their 'natural surroundings'. He argues that both routes have scientific method at their heart and that this method distinguishes these two approaches from all other methods of acquiring knowledge such as heuristic learning or experiential based learning. He further demonstrates that the scientific method constitutes a sliding scale from single variable controlled laboratory experiments at one end to surveys at the other. This reflects the observation made above that methodology should be seen more on a continuum than as a choice between poles. He argues that the trade-off between precision and contextual richness along this scale is situation dependant; but emphasises that the isolation of variables in laboratory conditions outside their natural environments does little to generate generalisable theory and pays scant attention to how that variable is impacted by all the other variables in its real setting.

Thus, Bonoma separates out quantitative and qualitative research methods while simultaneously graduating them along a scale from one to the other. However, Gable presses the case for combining these two methods into one approach citing the combination of qualitative case-study and quantitative survey methods as an example.[43] His own literature survey indicates evidence for a tolerance of 'methodological pluralism' as well as recognition of appropriate method, where circumstances rather than any assumed supremacy of research is the arbiter. He adds that the impact of personal bias of the researcher is also critical. However, he rather weakly concludes that the case for combinative methods is strong, but adds that actual research designs that incorporate both methods are rare. He also attempts to distinguish Yin's interpretation of case-study and survey combined, where a survey may be used as a data collection method for an embedded unit of analysis, from a combined case-study and

survey approach, where both are applied to the same unit of analysis. The distinction remains unconvincing but does serve to highlight the increasing combination of approaches that researchers are justifying, as well as 'bolder' moves away from the pure science, quantitative based approach.

Finally, Cavaye declares the case-study to be jack *and* master of all trades when he shows that case-study methodology can: "be conducted either from a positivist or interpretivist viewpoint; be hypothesis testing or theory building; deductive or inductive; qualitative or quantitative; and single or multiple in nature."[44] He adds, as if the variety is not already sufficient: "(I)t can be anything in between these [two] extremes in almost any combination".[45] He argues, far beyond Yin, that the case-study strategy is versatile and pluralistic and particularly appropriate when theoretical knowledge on a phenomenon is limited or when the need for capturing context is important. He concludes that: "there are few, if any, research situations where case research would be inappropriate." This author rests his case for the case-study approach in regard to the research question in this thesis: that the contribution of open source exploitation can be described by a set of high order factors. It is worth adding a word of caution from McCutcheon and Meredith:[46]

> "Case-study research can only go so far, of course. In other words, it is not necessarily an efficient form of research. However, more efficient methods must constantly rely on such techniques as case-study research to ensure that our theories, experiments and advice to managers do not become detached from reality."

3.1.6 Differentiating case-study as strategy from ethnography as methodology

It is worth differentiating case-study strategy as guide to discrete research design, from the logic and philosophy of ethnographic and grounded-theory methodology that might guide strategy. Ethnographic research implies extended periods of participant observation and involvement with the study subject. For practical reasons to do with the specific target of this research, such an extended access is discounted as strategy.[47] However, the principles of participant observation as methodology are relevant.

Grounded theory oscillates between inductive and deductive thought; the researcher filling in missing areas of information and conclusions based on logic.[48] It can be argued that this is what the author is attempting, albeit in just two or three iterative stages. Grounded theory also emphasises the need for the researcher to enter the research setting with as few preconditions as possible.[49] For this reason the author chooses case-study as strategy over grounded theory, as prior involvement with the intelligence community together with preliminary observation might inevitably lead to preconditions or prejudice. However, as Collis and Hussey note, having recognised any such prejudices: "(their) validity can be questioned and (they) no longer remain a bias".[50] Eisenhardt infuses case-study strategy as basis for research design with much grounded theory principle as guiding methodology.[51] This closely represents the author's approach.

3.1.7 Data collection methods

Having established case-study as a strategy most likely to deliver an optimum route by which to address the research question, it remains to determine how best to extract appropriate data from the cases. Again, there is a choice regarding the usefulness and appropriateness of alternative procedures. Quantitative methods such as questionnaires, surveys or data banks are ruled out from the start. Statistically they will be rendered meaningless given that the population size is not significantly different from the number of case-studies engaged with. Theoretically, and more importantly, they are less likely to lend meaningful understanding to the subject than qualitative methods. Qualitative methods include interviews, observation and diary methods supplemented by supporting techniques such as 'repertory grid', 'protocol analysis', cognitive mapping and group or focus interviews. These supporting techniques were considered broadly too reductionist for the nature of this research, characterised more by exploration and description than explanation and prediction, or, like diary methods, simply inappropriate for the nature of the case-studies and subject matter.

It is important to recognise that qualitative and quantitative methods are not mutually exclusive nor do they have to deliver specifically qualitative or quantitative results. It

is how the results are used for analysis and interpretation that finally decides whether they are used for statistical (quantitative) or understanding (qualitative) purposes.[52] Van Maanen describes qualitative data collection methods as:[53]

> "An array of interpretive techniques, which seek to describe, decode, translate and otherwise come to terms with the meaning, not the frequency, of certain, more-or-less naturally occurring phenomena in the social world".

The two research methods considered for data extraction are 'semi-structured interview' (interview) and 'participant observation' (observation), where interview is likely to be the predominant data collection method throughout. Observation is particularly useful during the preliminary model stage as a powerful tool to increase familiarity with the case-studies and the specific language and nuances of their various contexts. Semi-structured interview is then further directed at case-study data collection in order to develop the preliminary model. It is designed to link the informants to the variables within each case and record the differences in those variables across both the informants and the case-studies. It is likely that observation will inevitably co-exist alongside interview in this more formalised data collection phase. Again, both are utilised in the final model confirmation phase, with interview predominating the data collection and observation predominating the context.

Participant observation

Participant observation is rooted in anthropology. Originally it involved 'living-with' tribes in remote areas as a way to record and understand their behaviour. Contemporary organisations are effectively 'tribes'; thus participant observation has, unsurprisingly, migrated from anthropology to management science becoming an effective research method for revealing their customs and practices. Junkers classifies the technique into four distinct options: complete participation, participation as observer, observer as participant and complete observer.[54] Easterby-Smith *et al* have translated this original classification for more modern management and organisational-oriented research:[55]

- **Researcher as employee.** As its title suggests the researcher operates as an employee, either completely covertly even to the organisation or with the connivance of one or two members of staff for access but not the informants or object of study. Total immersion is designed to lead to deepest insight. This version of the technique has three key drawbacks. First, it may prove ethically and emotionally challenging for the researcher to be 'informing' against work colleagues. Second, the risk of jeopardising the research on discovery is high. Third, there is a considerable physical challenge to work and then conduct subsequent research effort in the hours available.
- **Research explicit.** The researcher's presence within an organisation is negotiated in advance and known to all. This presence is usually over an extended or continuous period. The beneficial insights of this approach reflect those of complete participation but without the ethical dilemma. Two key challenges are important for the researcher to overcome. First, gaining access, where more than one party now has an interest by being aware of the research process, can become more difficult. Easterby-Smith *et al* cite a case, where a researcher experienced considerable delay as those granting access debated the relative merits of the research.[56] Second, gaining trust from all in the study becomes very important to ensure the best possible opportunity for openness, honesty and thus richness from the respondents.
- **Interrupted involvement.** Here the research remains explicit but rather than a continuous longitudinal exercise it becomes a sporadic one. Equally, the researcher is less likely to participate in any of the work of the target organisation. It is usually combined with interview technique and as such seems most fitting to this research study.
- **Observation alone.** Again, as its name suggests this variation is purely observation. There is no participation in the work and there is no combination with interview. Indeed it is highly objective and remote. This degree of detachment from the subject seems almost positivist in design and hardly likely to create insight and understanding. It is not considered further.

Interestingly, the author's own intelligence experience concurs with these variations. The author has conducted each of them in previous work albeit by different name. The

main deciding point was usually one of time constraint. Covert activity takes considerable time to establish and even then key information might never present itself. And, when it does, it can be so devoid of context that its meaning is lost. Equally, pure observation is a technical intelligence method that is designed to be devoid of influencing context (objective) from both the target and collector's (researcher's) point of view. However, it is usually quicker to achieve. Quite often, the straight question to someone who knows, even if he knows the researcher's position, can illicit a most useful answer. It is no surprise that intelligence itself utilises all four of these varieties in combination on one target; something not detailed in the literature.

Interviews

In-depth interview is the most fundamental of all qualitative data collection methods.[57] The difficulty is knowing how much structure and complexity to put into the questions. The more formal, structured and simple the questions, the nearer one gets to a positivist questionnaire or survey. The more open and detailed the questioning the more meaningful and insightful the responses are likely to be. Additionally, face-to-face interviews present the interviewer with the opportunity to identify non-verbal clues.[58] Burgess summarises the importance of interview as: "(T)he opportunity for the researcher to probe deeply to uncover new clues, open up new dimensions of a problem and to secure vivid, accurate inclusive accounts that are based on personal experience".[59]

In order to ensure that meaningful insights do emerge from the research then care has to be taken in constructing the interview framework. Easterby-Smith *et al* highlight seven influences that the literature considers crucial:[60]

- **Structure.** Somewhere between a rigorous questionnaire and a completely open-ended conversation lies the semi-structured interview. Semi-structured formats are useful when it is necessary to understand the constructs that the interviewee uses as a basis for opinions and beliefs about a situation, thereby developing an understanding of the interviewee's world. The advantages of a semi-structured interview over structured or unstructured is that while all the subject areas of the research framework

are adhered to they also allow for deviation down alternative, better lines of enquiry to explore other emergent themes and patterns. Nothing is ruled out and everything is ruled in. Given the aim of this research and this data collection stage is to refine theory from generated then semi-structured interview seems neither too rigorous nor too open-ended.

- **Interview skills.** Interview skills are more about understanding the interviewee's motives and creating the opportunity for the interviewee to articulate views than specific techniques of the interviewer. As Mangham has shown, a positivist approach to qualitative data collection is invalid.[61] The way people construct meaning is more critical than the number of times they say it. The interviewer needs to be a good listener, needs to know what is relevant and important, needs to be perceptive to changing lines of enquiry, and needs to be aware as much about what is not said as is said. The interview needs to be 'remembered' by written or taped record. The interview should be 'tested' against the respondent by summarising and offering the summary for checking by the interviewee.
- **Social interaction.** Both interviewer and interviewee can make judgements that influence the research from their social interaction at interview. Essentially, this is a reflection of trust in the interviewer by the interviewee. The result can range from unwitting misinformation to deliberate disinformation or lying. The recognition of non-verbal signals can help minimise these effects as can complexity of interview that creates deliberate contradiction. More importantly the creation of trust and interviewee relevance is imperative.
- **Trust.** Trust is difficult to engender. Easterby-Smith *et al* indicate that: knowing something about the target organisation, establishing an appropriate point of entry ('gatekeeper') with credibility, and using appropriate language with the case-study informants will all help.[62] They also suggest that with regard to data collection; it need not all happen in one go at the expense of building up dialogue over a longer period. Finally, like Miles and Huberman (discussed below), they recommend interviewing on 'neutral territory'.[63]
- **Interviewee relevance.** Where an interviewer can demonstrate interest in and commitment to case-studies and informants, this will help generate relevance to the interviewees. Equally, interviewees can experience a sense of usefulness as well as

gain improved understanding of their own organisation, which all contributes to relevance. Finally, involving the participants in review and checking procedures are not just 'ploys' to gain compliance but engender relevance and validation.

- **Interview bias.** Bias is dealt with more generally below; but the imposition of the researcher's own frame of reference on the interviewee presents a real dilemma. Using open questions tends to reduce the incidence of bias but open questions do not necessarily derive the specific information required. Easterby-Smith *et al* suggest the use of probing techniques; the overriding rule being that probing questions should never 'lead' the interviewee.
- **Interview ethics.** Interview ethics revolve around the micro-politics of target organisations and the agendas of all concerned, from those granting access to those being interviewed. Recognising that such influences can occur and understanding the issues they originate are probably the best defences to spotting it occurring in the first place. The nature of the developing relationship will temper or exacerbate this influence.

Interview questions

The semi-structured interview questions form the backbone of data collection and case-study construction. The interviews represent the mechanism by which the variables and informants are tied together within the case-study. Analysis of the data obtained by interview will establish how open source is exploited and, most importantly, reveal why it is done. In turn, it will also be possible to explore how the wider intelligence function is responding to it. Triangulation within and across the cases refines the model for its treatment beyond the preliminary stage. The refined model represents the answer to the research question, which might then be tested.

3.1.8 Qualitative data analysis

Data analysis methods should be appropriate to both the researcher's philosophical position and the data collected.[64] The researcher's philosophical paradigm has been firmly described above as phenomenological. The data collected in the research is

qualitative rather than quantitative. Hence the data analysis techniques will be pertinent to qualitative data.

Qualitative data analysis is considered more problematic particularly when compared to quantitative: the analysis process is less well described in the literature than collection;[65] distinction between collection and analysis is often unclear;[66] and qualitative data analysis techniques are not as readily acceptable as quantitative.[67] Overcoming these challenges requires three key steps: [68]

- **Data reduction.** Data reduction systematically streamlines data to facilitate the drawing and verifying of conclusions.
- **Data structuring.** Data structuring utilises an *a-priori* set of categories or structure into which data can be fitted. In this study the identification of key variables and the developing model of high order factors begins and reflects that process respectively. It is important to note that any tendency toward 'anticipatory data reduction', where data is ignored if it does not fit a constructed theoretical framework (research instrument), is acknowledged and avoided here. Such anticipation restricts richness and understanding.
- **Data detextualising.** Detextualising involves converting extended text into diagrammatic, illustrative or quantitative format for analysis and subsequent presentation.

Qualitative data can be analysed with quantifying treatments or non-quantifying treatments.[69] The intention is to allow recognition of pattern and repetition.[70] The outcome is to facilitate evaluation of the analysis.

Quantitative treatments include: 'content analysis',[71] and 'repertory grid technique'.[72] Non-quantitative treatments follow a general analytical procedure detailed by Miles and Huberman for dealing with qualitative data.[73] This procedure is similar to 'grounded analysis' of Easterby-Smith *et al*,[74] and the varieties of grounded analysis developed by Glaser, Strauss and Corbin from 1967 onwards. It is a systematic and methodically rigorous treatment of large volumes of collected data material, including:

- **Record.** Convert field notes into written record. Add thoughts and reflections by way of initial analysis.
- **Reference.** Reference all material collected to include who, when, where, how, why and any implications for the research. Create an index system for these references.
- **Code.** Code the data as early as possible to include variables, concepts and themes with examples of each as they emerge from the data.
- **Categorise.** Group the codes into smaller categories, compare new data as it emerges from the study and modify the codes and categories appropriately.
- **Summarise.** Summarise findings at appropriate stages. This aids analysis and highlights necessary modifications.
- **Generalise.** Use these summaries to create generalisations, which challenge existing theories or create new theories. In this particular study, model generation is the aim.
- **Iterate.** Continue the process until new theory is robust enough to stand the challenge of existing theory or new theory is constructed.

Non-quantitative treatments utilise the following analytical and presentational techniques: 'cognitive mapping', developed from Kelly's 1955 theory of personal constructs[75] through Ackerman, Eden and Cropper's 1990 'User's Guide'[76] into computer software such as *'cope'*, *'Ethnograph'*, *Atlas-ti'*, and *'NUD*IST'*; 'data displays' such as networks, matrices, charts and graphs;[77] 'grounded theory';[78] and 'quasi-judicial method' drawn from the judicial system whereby rational argument is used to interpret empirical evidence.[79]

Whether computer analysis is used or not, and Easterby-Smith *et al* are by no means convinced that it is essential,[80] computer analysis still ultimately depends upon the judgement of the researcher, from data input to conclusions drawn. Furthermore there is a tendency for computer analysis programmes to tend toward frequency rather than meaning.

Slightly confusingly Easterby-Smith *et al* describe most of quantitative and non-quantitative techniques described above as 'supplementary interview techniques'. [81] This confirms Collis and Hussey's problem of distinguishing data collection from data

analysis.[82] However, Easterby-Smith *et al* then go on to identify content analysis and grounded analysis as quantitative and qualitative data analysis techniques respectively, which accords with this author's understanding of their role.[83]

3.1.9 Evaluation of analysis

Ultimately the evaluation of analysis depends upon the data collected and the researcher's quality of interpretation. Everything else is geared-up to making these two elements as rigorous as possible. Lincoln and Guba suggest four criteria for evaluating analysis and thus the entirety of a phenomenological study:[84]

- **Credibility.** Credibility demonstrates that the subject of the research was correctly identified. It can be improved by the researcher's: prolonged involvement with the study, which Leininger describes as 'saturation' or immersion so that the researcher is fully conversant with the project;[85] persistent observation to achieve depth of understanding; triangulation of a variety of sources and data collection methods; and by continual peer de-briefing.
- **Transferability.** Transferability attempts to show that the findings are generalisable.
- **Dependability.** Dependability demonstrates that the research process is systematic and rigorous. Collis and Hussey add 'respondent validity' to evaluate the analysis of data.[86] This involves inclusion of the informants in reviewing the researcher's findings.
- **Confirmabilty.** Confirmabilty is the criterion for demonstrating that findings 'flow' from the data.

3.1.10 Criteria for judging quality of research design

Reliability, validity and generalisability are the three qualities that comprise research credibility and, which research design must satisfy. Collis and Hussey argue that if the same results emerge each time the research is repeated then the research is reliable.[87] Phenomenologically, research is looking for similar interpretation of the same

circumstances on different occasions or by different observers. Validity is the degree to which the research truly represents what is actually happening or demonstrates what the researcher says it does.[88] Phenomenologically, this is achieved by gaining as complete an access as possible to the phenomenon in order to maximise richness and understanding. Generalisability is concerned with attempting to come to conclusions about one thing based upon information derived from another.[89] Gummesson argues that in phenomenological studies, it is possible to generalise from one set of circumstances to a similar set of circumstances, which this study closely reflects.[90]

Such criteria are logical tests by which one can judge the quality of any given design utilising concepts such as trustworthiness, credibility, confirmability and data dependability. Again, these are strikingly similar concepts to the criteria for evaluation of intelligence sources. Indeed several articles in the literature review have refered specifically to the process of analysis in intelligence, which displays similarity in many areas to research methods.

Yin suggests that, because a research design represents a logical sequence, you can also judge the quality of any given design by certain logical tests.[91] He identifies four:

- "Construct validity - the establishment of correct operational measures for the concepts being studied.
- Internal validity - the establishment of a causal relationship, whereby certain conditions are shown to lead to other conditions, as distinguished from spurious relationships. (For explanatory or causal studies only).
- External validity - establishing the domain to which a study's findings can be generalised.
- Reliability - demonstration that the operations of a study - such as the data collection procedures - can be repeated, with the same results."

The internal validity test is not required for this study and is not discussed further. Yin goes on to suggest both case-study tactics and phase within the case-study that will ensure these conditions are met. These criteria are shown in Table 3.3 below.

Table 3.3: Case-study tactic and phase for design test

Test	Case-study tactic	Phase of research in which tactic occurs
Construct validity	• Use multiple sources of evidence • Establish chain of evidence • Have key informant review draft case-study report	Data collection Data collection Composition
External validity	• Use replication logic in multiple case-studies	Research design
Reliability	• Use case-study protocol • Develop case-study data base	Data collection Data collection

Source: Yin, 2003.[92]

3.1.11 Possible limitations of research method

The chosen research methodology contains a number of limitations. The most important aspects are reviewed below. Common to all social science research, it is impossible to control for the influence of ongoing developments either external or internal to the research. However, the orientation of the research is in discovering relevance towards long-term trends and implications for policy rather than reacting to spontaneous events.[93]

Bias

It is important to be aware of the potential for bias accruing as a result of the researcher's own observation and presence. Such bias is broadly distinguished into 'suspicion' and 'trust'. The former is a more severe version of the latter. Suspicion is aroused that the researcher is an 'informant' of the case-study organisation.[94] Trust is a virtue of the relationship formed between the researcher and the case-study organisation. It is unlikely to flourish in the presence of suspicion and is more difficult to establish by researchers 'external' to the case-study.[95] Miles and Huberman additionally describe two further aspects of bias: Type A and Type B.[96] Type A is that

bias, which emerges as a result of the researcher's presence and observation causing disruption to normal behaviour. Type B is that bias, which emerges as a result of the researcher being affected or influenced by the case-study. Both types can impact upon the research. Furthermore, each type can trigger the other. Easterby-Smith *et al* describe the various 'probes' that can control bias. [97] Miles and Huberman give guidance on the avoidance of bias for researchers observing and interviewing within case-studies. [98] The guidance is shown in table 3.4 below. With the exception of showing field notes to colleagues, all the points in the guidance were followed as closely as possible.

Table 3.4: Guidance on avoiding bias

Avoiding biases stemming from researcher effects on site	Avoiding biases stemming from effects of site on researcher
Stay as long on site as possible; spend time fitting into the landscape, and adopting a lower profile. Wherever possible use unobtrusive measures. Ensure that the intentions of the planned research are unequivocal and accessible for informants. Explain why you are there, what you are studying, how you will be collecting information, as well as what you intend to do with it. Consider co-opting an informant – asking that person to be attentive to the influence that you as a researcher has on the site and its inhabitants. Where possible interview off-site, preferably in a congenial social environment (café, restaurant, informant's home). This should help to reduce the thereat quotient and exoticism. Do not inflate the research problem in order to make it seem more important than it really is.	Avoid the 'elite' bias; include lower-status informants and people outside the focus of the study. Avoid co-optation or 'going native' by spending time away from the site; spread out site visits. Be sure to locate people with different points of view from the mainstream, people who are less committed to tranquillity and equilibrium. Keep thinking conceptually; translate sentimental or interpersonal thoughts into more theoretical ones. Consider finding an informant who agrees to provide background and historical information, and to collect information when you are off-site. Triangulate with several data collection methods. Do not overly depend on one source. If you sense you are being misled, try to understand why the informant would find it necessary to mislead you. Show field notes to colleagues. This may help establish that you are not being misled and that your field notes are focusing on the research problem. Keep the research question firmly in mind.

Source: Adapted from Miles and Huberman, 1994.[99]

Theory building from cases

The intensive use of empirical evidence can yield overly complex theory, which tries to encapsulate the full richness of the data.[100] Thus, researchers have to assess which are the most important relationships and which are superfluous. Conversely, building from cases may result in narrow, idiosyncratic or modest theory. While they may be testable, novel and empirically valid they remain theories about specific phenomena. Nevertheless they are likely to tie in well to broader theoretical issues.[101]

How many case-studies make a case

There is much debate about the optimum number of case-studies. Eisenhardt declares for between four and ten.[102] Hamel *et al* consider that it is not of paramount importance since no sociological investigation can be defined on the basis of that issue alone.[103] While Darke *et al* simply assert that there is no ideal number.[104] Intuitively it seems sensible that the more cases, then the greater the chance of replicating the logic of the research design, literally or theoretically, and increasing the sources of evidence.[105] However, the greater the number of cases then the greater the likelihood of increasing the number of impacting variables. Like much in research, the real world intervenes to force the striking of a balance.

'Absence of research' and 'action research'

A further limitation of the research methodology concerns the difficulty of knowing what would have happened in each of the case-studies had they not been subjected to research. This conundrum reflects Heisenberg's principle - that observation of a phenomenon changes the very status of the phenomenon being observed. The danger is that the researcher inadvertently becomes 'consultant'; for better or worse, but for a change nevertheless. Collis and Hussey recognise such a deliberate approach as a valid research strategy known as 'action research'.[106] Gummesson acknowledges the approach but argues that it can be likened to journalism and therefore prefers the term 'action science', which can be scientifically judged from a phenomenological rather than positivist point of view.[107]

The inability to extract the researcher from the case-studies creates problems in assessing what would have happened. This type of problem is not confined solely to phenomenological inquiry - evidence from other research strategies face similar dilemmas.[108] Although acknowledging this issue as a serious limitation, a researcher is only able to hypothesise about things, which are established. Thus, the researcher's principal job is not to speculate about what might have been but rather deal with 'what is' as evidence.[109]

Two potential pitfalls exist in regard to action research, which this study avoids. First, there is a conscious desire to change what is being researched. Second, the research is jointly agreed and conducted by the researcher and the researched. In this case it is not clear prior to the research that anything needs changing, and, beyond gaining access to the cases and common courtesy after that, there is little need to agree any combined research agenda. Inevitably, the cases will gain access to this write-up; what they do with it is up to them.

Ethical interviewing

Notwithstanding that 'need to know' and compartmentalisation is culturally ingrained into intelligence organisations it must be assumed that:

- Informants will 'confer' to some degree both within units and across units.
- Informants will come with bias and weighting in respect of their affinity and regard for the research subject.
- The author may unwittingly engender bias in the informants through research design and conduct of the research.

The case-study design and case-study protocol have been designed to reduce the likelihood of conferring. Triangulation of data within and across case-studies will mitigate the impact should it happen. Whilst 'conferring' may occur within units of analysis in any study it is less likely that it will occur across units of a study. With regard to bias in either/both the informant or researcher, interview techniques engendering trust and controlling social interaction are crucial.[110]

3.2 Part Two: Research strategy and design for this study

> "A research design is the arrangement of conditions for the collection and analysis of data in a manner that aims to combine relevance to the research purpose with economy in procedure."
>
> Selltiz, Wrightsman & Cook, 1976.[111]

3.2.1 Study approach

As was noted in the review of literature in Chapter Two, there is precious little research literature related to open source exploitation and very little that specifically describes how it contributes to the intelligence function as OSINT. The first part of this chapter has reviewed research methodology generally, and reconciled the author's 'worldview' (phenomenological) with the research needs of the project (case-study). Upon reviewing the literature on research methodology, one might be forgiven for coming to a conclusion that 'anything goes'. However, this would be to neglect some fundamental tenets underpinning research, which will intuitively and instinctively if not inevitably return the researcher to the path of rigor: why are you doing this research; what are you trying to find out; how will you go about it; what did you find out; and so what? This part details a precise course of action based upon case-study as strategy for the research design.

The research methodology for this study is phenomenological and qualitative. It is not an empirical approach in the sense that it is trying to prove something 'correct'[112] It is not quantitative in the positivist sense of generating irreducible formula. However, the research is attempting to generate theory or hypothesis, in the form of a model, by induction from data collection. Of course, Hume's conundrum that induction, no matter how vast the data set, is still no guarantee of a watertight theory is yet to be roundly refuted. Indeed, this author empathises with the logic of that argument. Fortunately, Popper, although no fan of induction, offers a glimmer of hope when he presented his 'falsifiability theory' by way of refutation, which broadly states that something is the case until proven otherwise. Yet, both neglect to recognise that part of the scientific method is as much sparked into life with the genesis of an idea in the true

sense of the word experimentation (if not sheer serendipity), than experiment in the sense of process. Theory generation and subsequent testing has to start somewhere.

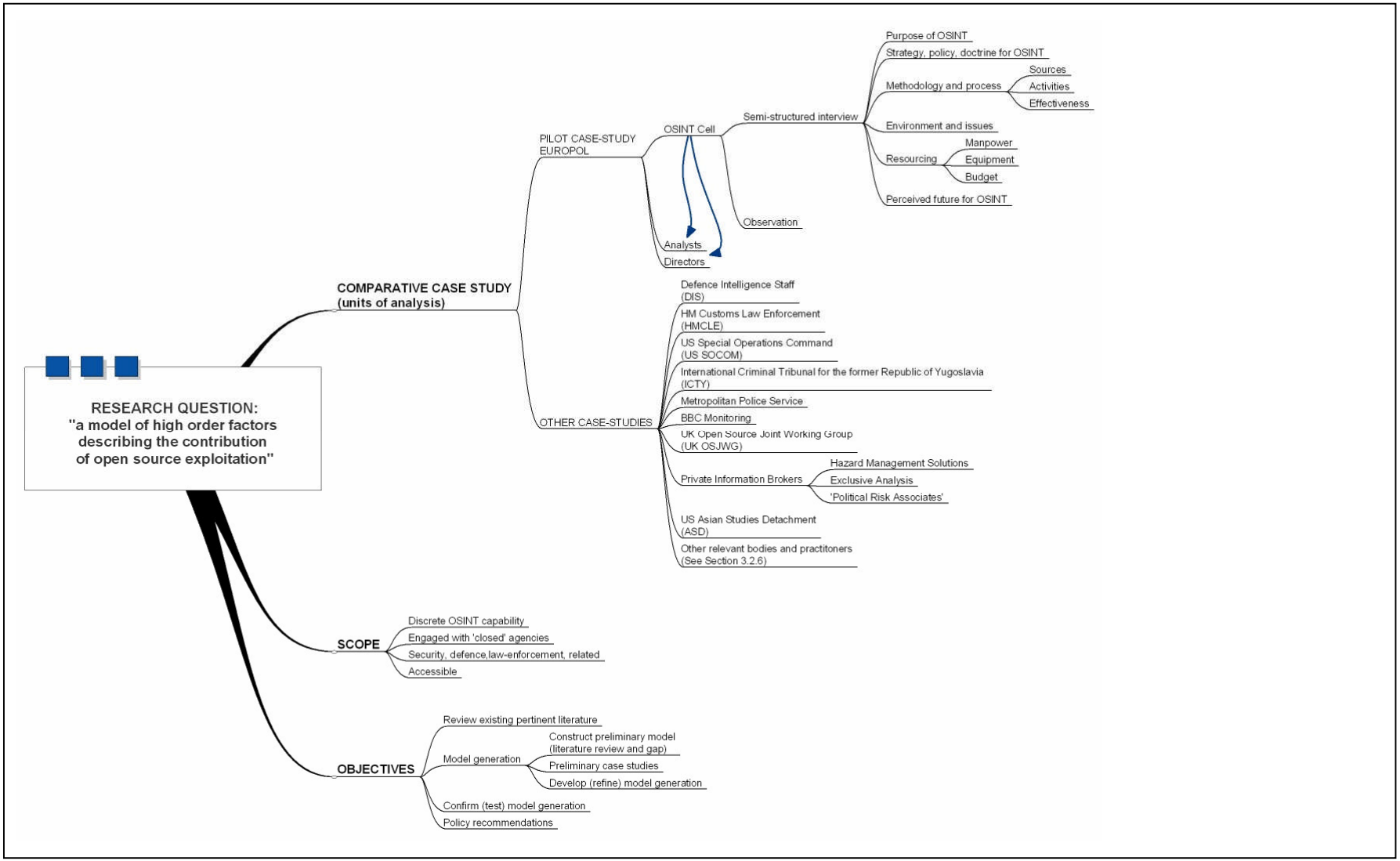
Theory generation in the form of a model of high order factors that describe the contribution of open source exploitation's contribution to the broader intelligence function is the question at the heart of this research effort. It is believed that the model derived in Chapter Four is valid as far as the research data and circumstances allow, in that it passes the falsifiability test within its own boundaries. It is hoped that the model might subsequently be exposed to a more deductive approach, where testing for generalisability and falsifiability might be more rigorous. Alternatively, the underlying assumptions, which focus the research into looking at intelligence from the open source point of view (rather than perhaps from the broader intelligence perspective), might be jettisoned for a different approach. Such an approach would not necessarily negate this research; rather, it would merely embark upon a different course starting with a different idea. Indeed, the final model produced here may very well be modified on the basis of subsequent research that encompasses a similar but alternative data set. This would be most welcome; but it is beyond the scope of this effort. Within its own boundaries, the constructed model is considered reliable because the subsequent research iterations repeatedly confirmed it. Thus, the methodological approach and subsequent model generation is considered a useful start point for subsequent research to build upon.

Of course, the research design is shaped by the detail of reality. This research was no exception. The case-studies were not as uniform as hoped for in the sense that they were not, for example, all uniformly 'all-source' intelligence organisations. Access to all the particular units of analysis within each case-study was not possible. Not all case-studies were as 'engaging' as each other. This is to be expected in social science research and arguably foolish to expect otherwise when the particular subject matter is current intelligence activity. The structure and culture of social constructs have as much to say about the outcomes of their efforts as an examination of the raw materials they work with. Suffice to say that those organisations keen and willing to engage, whether highly secrecy oriented or completely open, reflect a degree of mastery of their

discipline and perhaps more importantly for them the confidence of their customers and 'sponsors'.

In all of this it is imperative to maintain the aim of the study at the front of one's mind throughout the research process and particularly the analysis phase. Thus, data was collected from all of the types of units of analysis and across a wide variety of intelligence organisations. Arguably a self-selecting but entirely random selection of case-studies is as valid as one deliberately chosen. The significant point is that all of the case-studies have the most important factor in common; they all exploit open sources of information, and in theory they all have similar access to open sources of information, the same information, should they choose. It is what they make of it, how they exploit it, and to what purpose they put it that crucially explains why they should do it at all. Yet, the 'why' is what has been missing. A broad outline of the research design is shown at Figure 3.2.

Figure 3.2: Research design outline



Source: Author

3.2.2 Study process

Eisenhardt develops a 'roadmap' or study approach to theory building, which correlates well with Silverman's iterative induction process and Glaser and Strauss' grounded theory. [113] Defining a research question and *a priori* constructs helps focus the research onto the sort of data collected and how it is examined. That process is largely followed in this study and warrants expansion here as the guide for this design:

- **Getting started.** Ideally, Eisenhardt begins a research project as close as possible to no theory under construction and no hypothesis to test; but with the aim of building theory from tentative research questions and constructs. However, she acknowledges that all research requires a premise and *a priori* constructs. The research question here sets out to explore the contribution of open source exploitation to intelligence, in order that it might be described. Additionally, the research aims to analyse how this contribution might impact upon the conduct of intelligence. The *a priori* construct emerges from the review of literature and is then developed through the preliminary enquiries and refining case-study research.
- **Selecting cases.** Given that the research question is to describe the contribution of open source exploitation to intelligence, it is important to select case-studies where such contribution occurs. Essentially, this means an examination centred upon open source cells that feed into the broader intelligence function. This does not necessarily infer that such open source efforts are contained within the closed intelligence community. Increasingly, closed intelligence communities utilise open source exploitation that originates from many diverse sources outside the closed. Nor does it necessarily infer that the broader intelligence function is an all-source one. Open source is exploited within single-source agencies as well as within all-source ones. Furthermore national intelligence capabilities vary in their recourse to closed means. Accordingly, their reliance upon open versus closed sources will be different. It also does not infer that intelligence is something pursued exclusively by nation-states. International government organisations, the private sector, and non-governmental organisations are all aware of the necessity to optimise decision-making. Their information sources are more likely to lean upon open sources than

closed. Arguably, by its very definition, the recourse to open sources of information is essentially the same for every intelligence organisation. In theory, its exploitation should only be differentiated by the resource and skill applied to it, and the requirement for it. Thus, the 'why', the question for this research, should be common. However, the research also aims to examine the implication for the intelligence function conventionally understood as the nation-state effort. Thus, case-study preparation will preferably select organisations that have an established and discrete OSINT capability feeding into intelligence efforts supporting security, law enforcement, and defence, where their product is combined with closed intelligence. Ideally, this would be an open source effort contained within an all-source agency. Of course, the field is not so conveniently uniform. Thus the case-studies are principally selected from across the US, UK, and international intelligence communities, where a closed intelligence capability utilises open source exploitation for broadly public sector activity.

- **Crafting instruments and protocols.** The existing descriptors of open source exploitation found in the literature are united to form the basis of a model. This model is further developed and refined through qualitative data collection against case-studies. Finally, the model is tested against a single stand-alone open source organisation to conclude the research. Data collection methods will be semi-structured interview and participant-observation of key informants. This will be supplemented by continuing literature review and open-ended discussion with other OSINT and intelligence practitioners in order to provide comparative (contradictory or supportive) data. This in turn strengthens triangulation and subsequent recommendations for open source policy.
- **Entering the field.** Eisenhardt recommends the overlap of data collection with data analysis when building theory through case-study. She recommends the use of field notes: effectively, a running commentary on the research in order to capture impressions as they occur. This allows any new data collection opportunity to be used. Thus, the researcher can take advantage of the uniqueness of a case and the emergence of any new themes from it in order to iteratively improve the theory. This approach will be adopted in this research as it is most likely to create 'novel theory'.[114]

- **Analysing data.** Detailed case-study preparation will be undertaken for each study. Thus, each case might be reviewed as a stand-alone entity with its own patterns emerging prior to generalising across cases to find within-study and across-study similarities and differences.
- **Shaping hypotheses.** Eisenhardt recommends that there is constant comparison between data and constructs. The construct in this study is the induction of a model of high order factors, which in turn might form recommendations for policy regarding open source exploitation. Thus, shaping hypotheses becomes validation of the recommendations, which in turn, is achieved by checking that the recommendations fit with the evidence. Each recommendation will be examined for each case. Any recommendation supported by evidence may be considered a relationship and not so where the evidence is considered insufficient.
- **Enfolding literature.** Comparison with existing literature is an essential feature of this approach.[115] It strengthens triangulation and contributes towards Popper's 'critical rationalism' approach;[116] the continual search for data that falsifies a theory.[117] Contradictions require explanation. They promote either deeper insight for building theory or create unique features that can be set aside for further exploration.[118] Similarities with (and within) the literature strengthen confidence in the validity and generalisation of the research, particularly in this study, where a limited number of cases exist.
- **Reaching closure.** Eisenhardt identifies two issues critical to reaching closure: when to stop adding cases and when to stop iterating between theory and data.[119] This study closes off cases existing outside the boundaries highlighted in Chapter One (Figure 1.1). However, other examples of OSINT practice are investigated to give greater insight into the exploitation of OSINT. Iteration between theory and data should stop when the improvement to the theory or model is minimal.[120] In this case, the final single stand-alone case-study (the US Army's Asian Studies Detachment) represents closure, as it became clear that they confirmed the model rather added anything to it.

3.2.3 Choosing case-study as strategy

According to Yin's 'research strategy choice' (table 3.2 above), the research question lends itself most readily to case-study, survey and/or archival analysis strategies. Case-study methodology is considered the most applicable strategy for this research design because: it applies to 'how' and 'why' questions; it does not demand control of events and variables; it relates to contemporary events about which little or no research has been conducted; and it further allows for a longitudinal comparative analysis of practitioner development should that be necessary. This is considered to be a perfect fit for research into intelligence structures.

However, it is also worth articulating why other methods seem less obviously appropriate. Experiment is ruled out given both the researcher and subject's propensity towards the phenomenological together with the difficulty if not pointlessness of identifying and isolating key variables outside their natural setting. The research aim and objectives desire richness, insight and understanding rather than frequency.

Archival analysis is ruled out since the formal exploitation of open source information within the intelligence function is a relatively recent phenomenon. Furthermore, reference to intelligence archives of any note is prohibited by classification and time-bar. However, in years to come this may very well prove a most useful strategy. Indeed, there is already some pressure to generate such evidence demonstrating the efficacy of OSINT.[121] Certainly within intelligence agencies, open source cells collect case-study evidence to support their own position in relation to the crucial allocation of finite resource.[122] For research purposes, a worthwhile design might contrast historical decisions (revealed in the fullness of their time-bar) based upon closed information, against decisions that might have been made with OSINT at the time.[123] In many respects contemporary analysts do this now, obtaining their information from a variety of open and closed sources to challenge contemporary intelligence-based decisions: the 'failings' of 9/11 being a classic example.[124]

Survey is a possible research strategy. An investigation of an OSINT model might be based upon all-source intelligence analysts, whose numbers are indeed sufficient to permit a statistically significant quantitative assessment. It is ruled out theoretically because the overall research is qualitative in nature attempting insight and understanding rather than measurement, and practically because they simply do not have the time to respond genuinely to such efforts. O'Hara suggests that survey evidence is open to quite a few interpretations, not to mention a presupposition that respondents will tell the truth.[125] Survey, may prove a useful subsequent strategy for testing the final model as hypothesis. However, one would have to be careful of bias in such an homogenous set of units of analysis.

The research aim is to explore how the intelligence function is changing as a result of the exploitation of open sources, by addressing the research question: how precisely the exploitation of open source can be described to contribute to intelligence. Determining how open source contributes to the intelligence function will be achieved through the iterative development of a model that describes the treatment of OSINT within the intelligence community. Model generation is theory generation from data rather than hypothesis testing against data. The philosophy is one of understanding rather than measurement, qualitative rather than quantitative, inductive rather than deductive, pure rather than applied, exploratory and descriptive rather than explanatory or predictive, and knowledge creating rather than problem solving. When this research is triangulated with the literature survey and the author's own experience it will help develop a model for open source contribution, which will in turn allow exploration of how intelligence might be changing as a result. Thus, case-study is considered the most appropriate strategy to extract useful and relevant data in order to generate a model of the high order factors describing open source contribution (Chapter Four) pursuant to a subsequent analysis of its implications for the intelligence function (Chapter Five).

3.2.4 Case-study qualified

Case-study as strategy can be applied to research design in order to achieve several broadly distinct effects.[126] In this research the case-study strategy is descriptive and

exploratory rather than explanatory, experimental or serendipitous.[127] The descriptive aspect is reflected in the recording of case-study practices, which have never previously been recorded. The exploratory aspect is reflected in the preparation and comparison of case-studies that exploit OSINT in order to construct a model of its contribution to the wider intelligence function. The pre-existing research, empirical or literature-based, is considered insufficient and insubstantial to launch explanatory or causal case-study design into such a relatively new field with such a notably difficult product to access and evaluate quantitatively. Essentially, there is no working hypothesis to test. This case-study-based research constructs one and tests it.

For the sake of completeness, the only possible relevance of explanatory case-study might be to prove a negative via a 'null-hypothesis': that, contrary to the mostly anecdotal and circular reporting of the 80 percent OSINT contribution figure, in fact the contribution is perceived to be less than or more than that. This still does not get to an objective measurement of the truth or reality of its effectiveness as an intelligence tool. Although not without merit in its own right, it is discarded for a variety of reasons: the 'measure' of contribution would be hotly debated; and the chance of being in possession of all the necessary documents in such a contemporary study would be in such severe doubt, given the nature of secrecy, that any theory might merely be pertinent to those documents and thus neither theoretically or quantitatively generalisable. These restrictions from the outset reflect what Eisenhardt terms - 'weak theory'.[128] Notwithstanding the merit, the author has already articulated the view, supported by practitioners, that the contribution of OSINT to intelligence, expressed in this way, is a meaningless figure.[129] It is the meaningful outcomes of intelligence that are more important. Understanding how intelligence is changing as a consequence of the formal inclusion of OSINT might be more meaningful. The contribution of open source exploitation as input seems clearly significant.

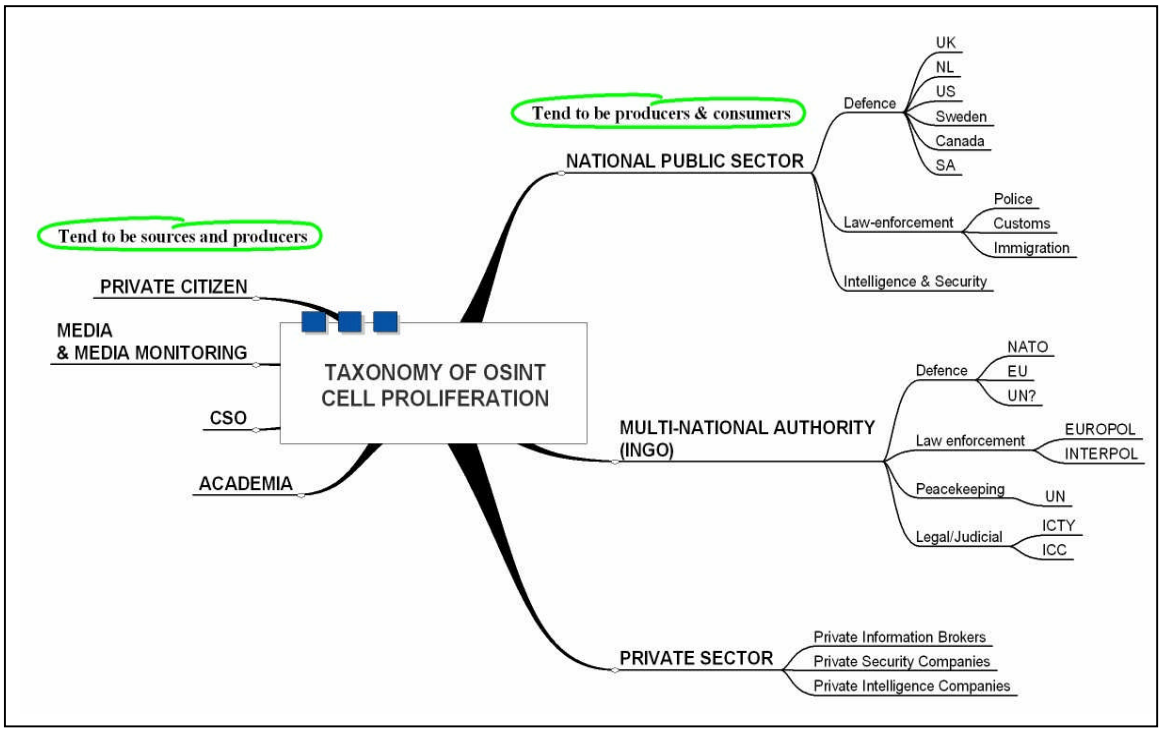
3.2.5 Selection of cases (units of analysis) to study

The selection of cases for this study has been most challenging: partly because of the practical and obvious reason of gaining sufficient access to the intelligence community

machinery, and partly because of defining the scope of the research within a sensible boundary. The latter has been the focus rather than the former.

Taxonomies of OSINT cells, which tend to form the core of OSINT exploitation, are indeed varied. The proliferation of open source cells as a constituent part of a nation-state's intelligence input to security, law enforcement and defence functions, although increasing, still remains limited in number. They also vary in maturity, resource available, and role. Furthermore a nation-state's security, law enforcement and defence functions are by no means the sole exploiter of OSINT. A broad taxonomy of open source cells is shown at figure 3.3 below.

Figure 3.3: Taxonomy of OSINT cell proliferation



Source: Author

The exploitation of OSINT can be categorised in a number of ways. One such might be the particular intelligence element of the security sector they serve: domestic or oversees security, law enforcement, or defence.[130] Yet, not all defence establishments, for example, pursue open source exploitation similarly. Sweden, Holland and Britain for example have all had OSINT cells centrally located within their respective ministries

of defence for a number of years. In recent years the UK in particular has seen the creation of a few open source exploitation efforts at formation and headquarters level in addition to the ministry effort.[131] Interestingly, the US experience is almost the reverse with open sources being exploited away from the DOD for many years, and, until 2006, no central DOD open source exploitation to speak of. They may be categorised by the sector of society that they serve: national intelligence agencies being broadly public sector; a private information brokerage (PIB) being broadly private sector. Yet both will contribute information to the other. Furthermore, an inter-governmental organisation (INGO) and a non-governmental organisation (NGO), are both likely to receive information from their respective nation-states, purchase it from PIBs, and establish their own capability all together. The International Criminal Tribunal, for example, has done all three. Alternatively, they may be categorised by the 'level' of institution in which they reside: intergovernmental organisations (INGO) such as NATO, EU, or EUROPOL have open source exploitation cells; national assets such as BBC Monitoring or the US Open Source Center are stand-alone open source organisations; cells within branches of an armed force such as the OSINT Exploitation Branch at US Special Operations Command, or a stand-alone PIB such as Oxford Analytica or Infosphere. Equally, they might usefully be categorised by culture or nation state: broadly Anglo-Saxon, European and Scandinavian or more specifically Australian, Dutch, and Swedish respectively. Finally, but not exhaustively, their historical, geographical, linguistic, social, political and cultural development might separate the context for intelligence, which OSINT contributes to, into broadly liberal or broadly authoritarian regimes.

In terms of a tight homogeneity then national defence organisations might well have proven to be an optimum boundary. However, their use of and relationship to closed sources varies dramatically. In terms of cutting edge then PIBs, NGOs, and media organisations might have demonstrated superior innovation. However, PIBs and NGOs tend to be single speciality or single issue specific. In some cases they are no more than one-man 'expert' bands. In some cases they prefer not to engage with a wider intelligence community and thus closed sources at all.[132]

Thus, a 'one-size fits all' taxonomy is not readily apparent. Moreover, such categorisations may ultimately produce a shallower model than one that cuts across them all and validates generalisability. Selecting case-studies from across the spectrum might illustrate common practice as well as diversity. Significantly, the one thing that unifies them is that they all exploit the same phenomenon - open sources of information. Indeed this may be the only truly significant and unifying commonality – the source material. However, their processes diverge, they have different objectives, different resources and different customers.

Interestingly, Berkowitz and Goodman might militate against a taxonomy approach for case-study selection.[133] On the one hand, they argue that, in the near future, boundaries between public and private sector intelligence creation will become increasingly blurred. On the other hand, they argue that, generally, leading edge technology is developed within the public sector rather than private sector for reasons of financial risk aversion.[134] It is the author's experience that public sector intelligence agencies, particularly US, are already engaged in integrating PIBs, not just as sources of information but also as centres of analysis. [135] This engagement includes tackling the difficult issue of reversing-out closed information from them to the PIBs for their use in analysis.[136] The important point to note here is that these 'changes' noted in the literature are being reflected in practice, and now noted in this research, precisely representing the change to the intelligence function that this research is interested in examining.

All these taxonomies may present useful future research projects but at this stage, given the lack of any research at all, it is considered prudent to ensure that research is actually undertaken. Notwithstanding the difficulty of taxonomy, all of the potential case-studies display some common characteristics: a dedicated open source exploitation effort, usually in the form of an 'OSINT cell'; their parent organisation or customers also deal in closed intelligence, single or all-source;[137] they are broadly engaged in intelligence product directed at security, law-enforcement and defence matters; they are engaged in work concerning global issues and the nature of their work is increasingly global; and they have a broad cultural homogeneity reflected in the Anglo-Saxon model

of the intelligence process that most developed western societies have adopted and developed. At the core of this model rests the development and maintenance of trust, which underpins the relationship between institutions of knowledge and power, through the establishment of audit and accountability procedures on behalf of those societies in whose name institutions of knowledge and power act.[138]

Collectively they comprise a sufficient number to encourage the model's construct validity and they all intersect to varying degrees with the more traditionally understood closed intelligence community. This latter qualification is in preference to any other common identity as it is the treatment of OSINT shaped by its relationship with intelligence generally that is at the ultimate aim of this research problem. Inevitably, the final choice of case-study has been tempered by ease of access. Collis and Hussey argue that finding representative case-studies is not as important as making sense of the data collected.[139] Case-study methodology can be aimed not only at statistical generalisation from a sample to a larger population, but also at theoretical generalisation, where it is proposed that one set of circumstances can generalise to another.[140]

3.2.6 Data capture: Case-study targets

Data for the model was collected in three deliberate phases from the following organisations, in which deliberate OSINT exploitation operations have been established in support of security, law enforcement and defence efforts:

Preliminary model:

- **European Police Office (EUROPOL)**. EUROPOL's open source effort was established in the mid-1990s until 2006, when it was closed down. It was a centralised effort, again consisting of around five personnel, who conducted all open source exploitation themselves. This case-study was effectively the pilot for the research project. An initial visit was made: to gauge issues of access; to refine the questions (see Appendix A) and semi-structured interview technique; to sense the

level of interest in the research, and to sense the general response to the researcher. Having made considered adjustments, a subsequent visit was made at a later time with different interviewees and sections.

- **UK Defence Intelligence Staff (DIS)**. The DIS open source cell was similarly established in the mid-1990s, is a centrally located resource, has had a staff of around five personnel at any one time, and whose operation was largely outsourced to a private contractor until 2006.
- **BBC Monitoring**. BBC Monitoring currently forms part of the Global News Division of the BBC.[141] It has the characteristics of an independent, non-governmental organisation with both funding from UK government and income from commercial activity. In intelligence terms it is an open source effort in its own right. It was established in 1938 and currently directly employs a little more than four hundred people worldwide, some of whom work in their stakeholder organisations. It works, globally, in partnership with the US government OSC.
- **International Criminal Tribunal for the Former Republic of Yugoslavia (ICTY)**. The ICTY was established in 1993 as a result of UN Security Council Resolution 827 following violations of humanitarian law during the early Balkans conflicts. Its open source cell is a centrally located resource working on behalf of the prosecution. It has had a reasonably permanent staff of around five or six throughout. Its expertise and direction has migrated to other parts of the broader International Criminal Court system in the Hague.
- **UK Her Majesty's Revenue and Customs (HMRC)**.[142] The Customs' open source effort is centrally located with its law enforcement branch in Ipswich. It has a significant resource of approximately 80 collectors and analysts.
- **UK Metropolitan Police Service (MPS)**. At the time of researching, the MPS open source effort resided within one or two individuals.
- **US Special Operations Command (USSOCOM) Open Source Branch**. This US Armed Forces effort was established in the early 1990s and has largely attained its success and reputation due to the enthusiastic efforts of its present director. It is centrally located, no more than ten-strong; but, given the culture of its parent unit, has 'cracked' its communication responsibility across its organisation and migrated open source exploitation throughout its analysis effort.

In all cases, with the exception of HMRC, the head of the OSINT cell was interviewed, the OSINT operation observed, and conversations conducted with various members of the OSINT staff. In one case (EUROPOL) access was further granted to analysts during this preliminary stage. In the case of HMRC, OSINT practitioners were interviewed, but further access was not allowed. However, the author did meet with the then Head of Intelligence Analysis for HMRC. In three cases (EUROPOL, DIS and ICTY), the establishment was visited twice. All of these cases, with the exception of ICTY, are more engaged in closed intelligence activity than open source exploitation.

Model development:

- **Hazard Management Solutions (HMS)**. Hazard Management Solutions is a private information brokerage (PIB) exploiting open sources of information concerned with improvised explosive devices (IEDs). Established in 2001; during the course of the research it has grown from two to 40-plus personnel, with both public and private sector clients.
- **Exclusive Analysis (EA)**. Exclusive Analysis is another PIB exploiting open sources of information for the purpose of conducting geo-political analysis with particular concentration on political violence and legal/financial risk. It was established in 2001, incorporated in 2002, and now has approximately 35-40 employees centrally located in London with 'stringers' located globally.
- **'Political Risk Associates' (PRA)**.[143] PRA is the third of three PIBs engaged with throughout the course of this research. It is a single individual effort and has been since its inception in the early 1990s. It has both public and private sector clients for its open source exploitation of 'single-issue protest and pressure groups'.
- **UK Open Source Joint Working Group (OSJWG)**.[144] The UK's OSJWG was established in 2000 and publicly recognised in 2006. It was initially established to represent and discuss 'best practice' amongst the open source practitioners within the three agencies of the Single Intelligence Account. Today its 'membership' has expanded to reflect the widening remit of a broader intelligence community and now leads the intelligence community on open source exploitation.

- **UK Cabinet Office Assessments Staff - 'Open Source Champion'**. This position, established in 2005, represents the link between the professional practitioner intelligence community and policy, for open source exploitation. The post operates particularly closely with the OSJWG.

In all these cases, the principle means of intelligence or knowledge generation is almost entirely through the exploitation of open sources of information.

Model confirmation:

- **US Asian Studies Detachment (ASD)**. The ASD was established in Japan in 1947 following cessation of hostilities with Japan post WW II. While it is a US Army asset, it retains a degree of autonomy as a stand-alone open source exploitation effort in that (like BBC M, but unlike SOCCOM) it resides outside any intelligence agency; certainly physically, virtually hierarchically and almost financially. In very recent years it has become a model of, and focal point for, US DOD open source exploitation. Its entire resource of almost 100-strong personnel is centrally located rather than dispersed.

This case-study represents the most complete example of an open source cell dedicated exclusively to open source exploitation, supplying product to closed intelligence customers, whose decision and policy interests lie in security, law-enforcement, and defence issues of global significance, and who operate within the broad framework of the Anglo-Saxon intelligence model. The case-study turns out, not only to confirm the model of high order factors that the preliminary and development stages construct, but also serves to test the model for generalisability.

Supplementary data:

Notwithstanding the final case-study choice for development of the model, it is worth mentioning that data collection has been supplemented through regular contact of varying intensity with a range of open source exploiting organisations, together with a number of former and current intelligence practitioners, including the following:

- UK Foreign and Commonwealth Office Research & Analysis Division.
- UK Defence Academy Conflict Studies Research Centre (Director)
- UK Cabinet Office Assessments Staff Open Source Champion
- UK Cabinet Office Briefing Room - Crisis Management Intelligence Cell
- The Oxford Intelligence Group (Michael Herman)
- Open Source Solutions (PIB - Robert David Steele)
- UK National High-Tech Crime Unit (NHTCU)
- NATO/SHAPE OSINT Unit (Europe)
- European Union Defence Force OSINT Unit
- Virtual Information Center/Asia Pacific Network (VIC/APAN) US DOD Pacific Command (PACOM)
- Infosphere (PIB - Mats Bjore)
- South African Defence Force intelligence analyst
- UK Defence Academy Advanced Research Analysis Group (Director)

3.2.7 Data collection: Informants and variables

Chapter Four takes an *a priori* construct from the literature review, develops a model based upon the author's preliminary enquiries and observations, refines it against selected case-studies, and finally test it against a single case-study. This evolution is achieved by analysing data collected against key components of the model throughout its iterations. Data is collected about components from informants. The components will vary within and across the cases; thus they act like variables.

Variables are entities that change and whose change can be measured or observed.[145] In this study the data collected about the variables will vary across and within cases.[146] In the case of OSINT exploitation the literature review and primary observations combine to suggest key variables as:

- Inputs (suppliers and sources)
- Process (producers of OSINT - the OSINT cell)

- Outputs (requested and consumed by customers - usually analysts)
- Environment (directors and organisational structures and cultures)

Informants are entities from whom or from which data about the variables are obtained. The open source cell is clearly responsible for the process of generating OSINT. Open source cells have inputs - suppliers of source material - into their process. They create product for their customers - analysts - whose output becomes a further source of input to the wider intelligence process in terms of fulfilling the requirements of ***their*** customers. Both operate in an environment that is directed vertically - directors of intelligence collection, together with the organisational culture that surrounds them. Directors have a general but final responsibility for product leaving the intelligence process, which may or may not incorporate open source amongst other sources. Analysts have more specific responsibility usually direct to customers internal or external to their organisation. Directors are responsible for the credibility (or external validity) of the product created internally. Additionally, by virtue of experience if nothing else, directors may have greater contributions to make with regard to the wider context of open source exploitation and its future efficacy. All of these participants to the process are data informants about the variables. Thus the informants to the model are:

- The OSINT Cell itself - producers of OSINT - where the whole cell is treated as a single entity.
- Analysts - consumers or customers of OSINT amongst other sources and formers of input to the OSINT process
- Intelligence Directors - final responsibility and context.

The semi-structured interviews are designed to prime the evolution of the model. That is to say, develop the iterative acquisition of data that more closely represents the real world treatment of open source exploitation. Data will be sought against the key variables from the informants in order to understand the exploitation of OSINT, to interpret the treatment of OSINT, and thus help refine the model. While the variables remain - inputs, outputs, process and environment - it was anticipated that the response

from informants with regard to the variables would vary within and across cases. Thus, in all of the engagements, the author used a common template of questions to guide open discussion (see Appendix A). The data collected was then compared within and across cases, represented by Table 3.5 below.

Table 3.5: The relationship between cases, variables and informants

CASE-STUDY / **Informants:**	**Variables:**	INPUTS	PROCESS	OUTPUTS	ENVIRONMENT
OSINT CELL					
CUSTOMERS/ANALYSTS					
DIRECTORS					

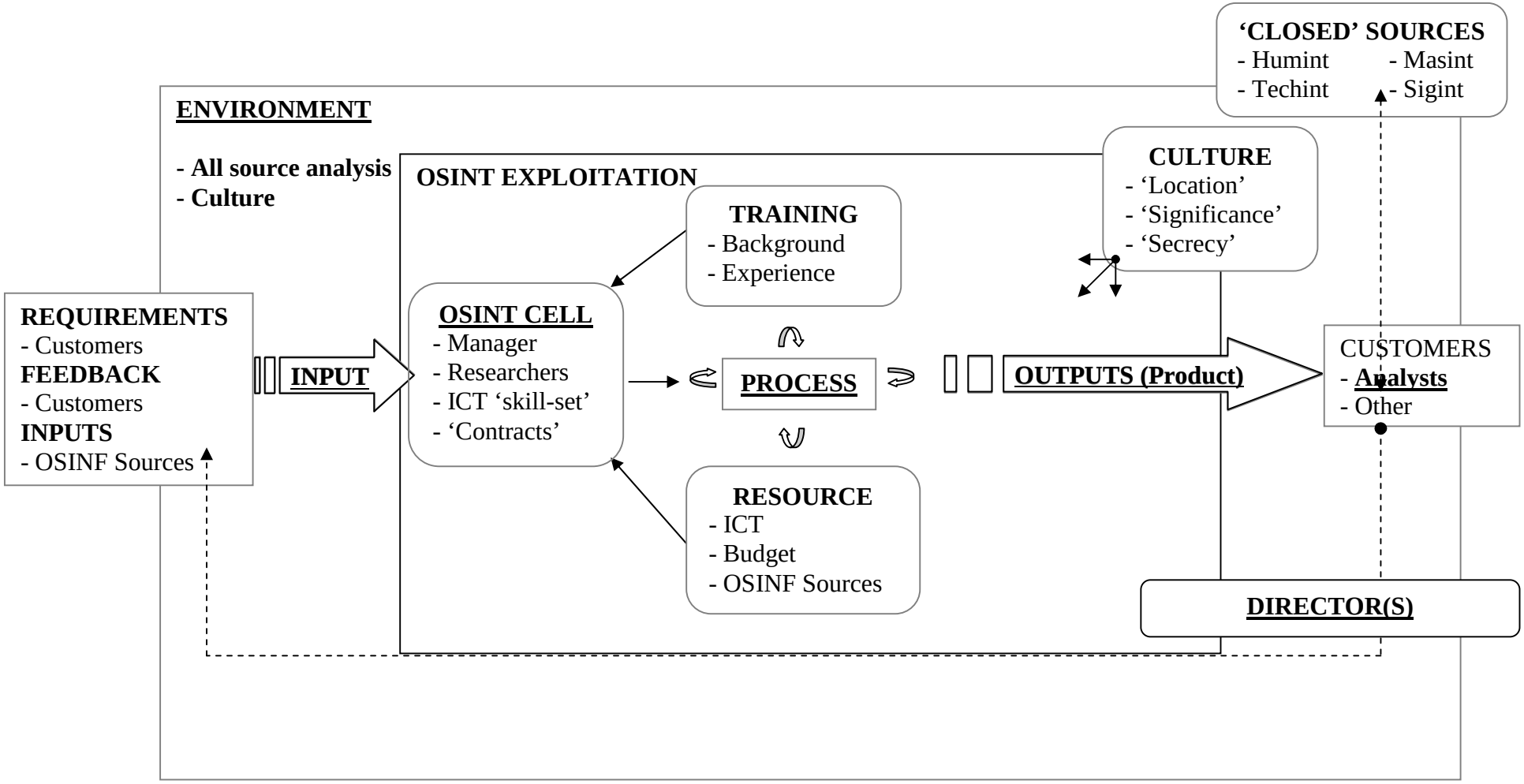
Source: Author

The aim was to elicit from the respondents their understanding of open source exploitation - what it means to them, how they do it, who does it, when it is done, where it is done, and, most importantly, why. This data was then compared and assessed in order to derive common high order themes or factors that describe the contribution of open source exploitation to the broader intelligence function. Having established these high order factors, the research might test them against other case-studies and begin to examine further, notions of effectiveness and implications for policy. Initially, it was considered that deriving a model of these factors would be a sufficient research achievement on its own and that testing the model might be a separate research effort. However, as the iterative examination of case-studies delivered repetitive descriptions of these factors, rather than new insights, what Eisenhardt describes as 'theoretical saturation',[147] it became apparent that the research could begin testing for generalisability too.

Figure 3.4 below outlines the system of informants and variables pertinent to the exploitation of OSINT. From the researcher's point of view, all interviewees were assured that interview notes would be anonymously attributed to the organisation rather

than the individual. In some cases, where senior officials' names are already in the public domain precisely because of their connection to the intelligence community, and open source exploitation in particular, they are named. Because of the nature of the case-study environments, it was impossible to tape-record interviews. However, all interviewees were content for notes to be taken, and in all cases the author transcribed these notes immediately after the interview was concluded. In the preliminary findings phase, some of the interviewees were presented with summaries for correction and comment.[148] From the model development phase onwards, all case-studies were presented with summarised notes for correction and comment. In the model confirmation phase (the ASD) all interviewees were also presented with the raw transcribed notes for correction and comment. All of the interviewees and case-studies supplied with these returns responded. The ASD interviewees commented extensively. Where a continuous but sporadic and less intense relationship existed there was no such checking of material.[149]

Figure 3.4: Informants and variables pertinent to the exploitation of OSINT



Source: Author

3.2.8 Research weaknesses

There was understandable concern at the outset that, given the absence of any other supporting research combined with the difficulties of access to case-studies, not enough data would be derived to be confident of presenting a generalisable model rather than merely a further testable hypothesis. However, the model eventually derived is considered to be reliable and valid as well as potentially generalisable given the final case-study against which it was tested. With a theory or model building approach by iteration, as identified in grounded theory by Glaser and Strauss and supported by Eisenhardt in case-study, theoretical generalisation to the 'similar' is possible.[150]

Arguably the final part of this research conducted at the ASD might be interpreted as positivist: testing a hypothesis that the generated model is or is not correct. Regrettably, the sample size against which to test the hypothesis is not that different from the known wider population. Statistically the generalisation would be meaningless in such a positivist sense. However, in a phenomenological sense, and in a context of ever increasing open source exploitation, it is considered a reliable method of inferring from one set of circumstances to another, potentially increasing, set.

3.2.9 The generation of intelligence theory by research

It is ironic that, near the point of completion and writing up of this thesis, in which mention has already been made of Johnson's call for an intelligence theory in the absence of one, Gill and Phythian begin to offer one.[151] Their 2006 book aims towards a theory of, and framework for research into, intelligence. Furthermore, they offer a framework for the conduct of research into intelligence, which highlights three key points:[152]

- The significance of the social-construction of knowledge
- The significance of the interplay between theoretical approach and empirical study
- An awareness of the larger picture

If the arrival of this extremely useful work in the twilight of this research effort is on the one hand somewhat frustrating, on the other - by way of confirmation of how this work was conducted - it is most comforting. All three elements are incorporated into this research, particularly a theoretical abstraction beyond the empirical research, which can be found in the analysis and discussion in Chapter Five.

3.3 Summary

Having examined the literature's view of the contribution of OSINT exploitation, it is clear that, while open source exploitation is an acknowledged contributor towards the broader intelligence function, it has only been partially explained as to why and how. It is possible to discern in the literature the beginnings of such an explanation, which might be incorporated into the description of high order factors at the outset. However, this handful of passing statements on open source contribution has little or no evidence behind it beyond the undoubted experience of the authors. Thus, this gap exposed by the literature should be filled in order to precisely explain how and why open source exploitation contributes to the intelligence function, as well as contribute to a broader development of a theory of intelligence.

This research is very firmly aimed at answering the 'why' and 'how' by posing a research question: how can the contribution of open source exploitation to the broader intelligence function be described. It proposes an hypothesis that a set of high order factors might collectively form a model that describes that contribution. It then constructs a model based upon data collected from cases studies of organisations that produce and consume open source intelligence. The model of contribution then precipitates analysis and discussion of the impact upon the conduct of intelligence. The next chapter reveals how the model was constructed from the data collected.

References and Notes:

[1] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *Management Research: An Introduction*, (Second Edition), London: Sage Publications, p.13.

[2] From "A Scandal in Bohemia." By (Sir) Arthur Conan Doyle. 1891.

[3] Collis, J., Hussey, R., 2003, *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, (Second Edition), New York: Palgrave Macmillan, pp.1-20..

[4] Yin, R.K., 2003, *Case Study Research: Design and Methods*, (Third Edition), London: Sage Publications.

[5] Pure research is also known as fundamental or basic.

[6] Collis, J., Hussey, R., 2003, *op cit*, pp.14-15..

[7] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[8] *Ibid*, p.27.

[9] *Ibid*, p.27.

[10] Gray, J., 2002, *Straw Dogs: Thoughts on Humans and Other Animals*, London: Granta Books.

[11] Habermas, J., Shapiro, J.J., (Trans), 1986, *Knowledge and Human Interests*, London: Polity Press; Collis, J., Hussey, R., 2003, *op cit;* Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[12] Smith, J.K., 1983, 'Quantitative versus Qualitative Research: An Attempt to Clarify the Issue', *Educational Research*, March, pp.6-13, p.10.

[13] Grayling, A.C., 2003, *Life, Sex and Ideas: The Good Life Without God*, Oxford: Oxford University Press, pp.231-233

[14] This is the direct quote from Heisenberg's February 1927 letter to Wolfgang Pauli at Hamburg University.

[15] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit*, p.32.

[16] *Ibid.*

[17] Cavaye, A., 1996, 'Case Study Research: A Multi-Faceted Research Approach for IS', *Information Systems Journal*, 6, pp.227-242.

[18] Easterby-Smith, M., Thorpe, R., Lowe, A., 1991, *Management Research: An Introduction*, (First Edition), London: Sage Publications.

[19] Morgan, G. , Smircich, L., 1980, 'The Case of Qualitative Research', *Academy of Management Review*, 5, pp.491-500.

[20] Collis, J., Hussey, R., 2003, *op cit*, p.52.

[21] *Ibid*, p.52.

[22] *Ibid*, p.53.

[23] Van Maanen, J., 1983, *Qualitative Methodology*, London: Sage.

[24] Ormerod, P., 2005, *Why Most Things Fail: Evolution, Extinction and Economics*, London.

[25] *Ibid.*

[26] Collis, J., Hussey, R., 2003, *op cit.*

[27] *Ibid*, p.60.

[28] Van Maanen, J., 1979, 'Reclaiming Qualitative Methods for Organizational Research: A Preface', *ASQ*, pp.520-526.

[29] *Ibid.*

[30] Yin, R.K., 2003, *op cit.*

[31] *Ibid*, p.5.

[32] *Ibid*, p.5.

[33] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[34] Collis, J., Hussey, R., 2003, *op cit.*

[35] McCutcheon, D.M., Meredith, J.R., 1993, 'Conducting Case Study Research in Operations Management', *Journal of Operations Management*, 11, 239-256, p.252.

[36] Cavaye, A., 1996, *op cit*; Gable, G., 1994, 'Integrating Case Study and Survey Research Methods: An Example in Information Systems', *European Journal of Information Systems*, 3, 2, pp.112-126; Bonoma, T.V., 1985, 'Case Research in Marketing: Opportunities, Problems, and a Process', *Journal of Marketing Research*, 22, May, pp.199-208.

[37] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit*, p.49.

[38] Miles, M., Huberman, M., 1994, *Qualitative Data Analysis: An Expanded Sourcebook*, (Second Edition), London: Sage Publications.

[39] Glaser, B.B., Strauss, A.L., 1967, *The Discovery of Grounded Theory*, Chicago: Aldine.

[40] Eisenhardt, K.M., 1989, 'Building Theories from Case Study Research', *Academy of Management Review*, 14, 4, pp.532-550.

[41] *Ibid, p.536.*

[42] Bonoma, T.V., 1985, *op cit.*

[43] Gable, G., 1994, *op cit.*

[44] Cavaye, A., 1996, *op cit.*

[45] *Ibid*, p.228.

[46] McCutcheon, D.M., Meredith, J.R., 1993, *op cit*, p.252.

[47] Werner, O., Schoepfle, G., Ahern, J., 1987, *Systematic Fieldwork: Foundations of Ethnography and Interviewing*, Newbury Park: Sage.

[48] Glaser, B.B., Strauss, A.L., 1967, *op cit.*

[49] Glaser, B., 1978, *Theoretical Sensitivity*, Mill Valley: Sociology Press.

[50] Collis, J., Hussey, R., 2003, *op cit, p.74.*

[51] Eisenhardt, K.M., 1989, *op cit.*

[52] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit*, pp.85-147.

[53] Van Maanen, J., 1983, *op cit*, p.9.

[54] Junkers, B. H., 1960, *Fieldwork: An Introduction to the Social Sciences*, Cambridge; Cambridge University Press, as cited in: Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[55] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[56] *Ibid*, p.112.

[57] *Ibid.*

[58] *Ibid.*

[59] Burgess, R., 1982, *Field Research: A Source Book and Field Manual*, London; Routledge, p.107.

[60] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[61] Mangham, I., 1986, 'In Search of Competence', *Journal of General Management*, 12, 2, pp.5-12.

[62] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[63] Miles, M., Huberman, M., 1994, *op cit.*

[64] Collis, J., Hussey, R., 2003, *op cit.*

[65] Morse, J.M., 'Emerging from the Data: The Cognitive Processes of Analysis in Qualitative Inquiry', in: Morse J.M., (Ed), 1993, *Critical Issues in Qualitative Research Methods*, Thousand Oaks: Sage, pp.23-43.

[66] Collis, J., Hussey, R., 2003, *op cit.*

[67] Robson, C., 1993, *Real World Research: A Resource for Social Scientists and Practitioner-Researchers*, Oxford: Blackwell.

[68] Miles, M., Huberman, M., 1994, *op cit.*

[69] Collis, J., Hussey, R., 2003, *op cit;* Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[70] Lindlof, T.R., 1994, *Qualitative Communication Research Methods*, Thousand Oaks: Sage.

[71] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit;* Silverman, D., 2004, *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*, (2nd Edition), London: Sage.

[72] Taylor, D.S., 1990, 'Making the Most of your Matrices: Hermeneutics, Statistics and the Repertory Grid', *International Journal of Personal Construct Psychology*, 3, pp.105-119; Stewart, V., Stewart, A., 1981, *Business Applications of Repertory Grid*, Maidenhead: McGraw-Hill.

[73] Miles, M., Huberman, M., 1994, *op cit.*

[74] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit*, pp.122-124.

[75] Kelly, G.A., 1955, *The Psychology of Personal Constructs: A Theory of Personality*, as cited in: Collis, J., Hussey, R., 2003, *op cit.*

[76] Ackermann, F., Eden, C., Cropper, S., 1990, *Cognitive Mapping: A User Guide*, as cited in: Collis, J., Hussey, R., 2003, *op cit.*

[77] Miles, M., Huberman, M., 1994, *op cit.*

[78] Strauss, A., Corbin, J., 1998, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (Second Edition), London: Sage Publications.

[79] Bromley, D.B., 1986, *The Case Study Methodology in Psychology and Related Disciplines*, Chichester: Wiley, as cited in: Collis, J., Hussey, R., 2003, *op cit.*

[80] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[81] *Ibid*, p.95.

[82] Collis, J., Hussey, R., 2003, *op cit.*

[83] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[84] Lincoln, Y., Guba, E., 1985, *Naturalistic Enquiry*, Newbury: Sage.

[85] Leininger, M., 'Evaluation Criteria and Critique of Qualitative Research Studies', in: Morse J.M., (Ed), 1993, *Critical Issues in Qualitative Research Methods*, Thousand Oaks: Sage, p.23-43.

[86] Collis, J., Hussey, R., 2003, *op cit.*

[87] Collis, J., Hussey, R., 2003, *op cit.*

[88] Coolican, H., 2004, *Research Methods and Statistics in Psychology*, London; Hodder & Stoughton.

[89] Vogt, W., 1993, *Dictionary of Statistics and Methodology*, London: Sage Publications.

[90] Gummesson, E., 2000, *Qualitative Methods in Management Research*, London: Sage Publications.

[91] Yin, R.K., 2003, *op cit.*

[92] *Ibid*, p.34.

[93] Durodie, W., (Ed) 2005, 'The Domestic Management of Terrorist Attacks', London: Report No: L147251003, available from author.

[94] Adler, P., Adler, P., 'Observational Techniques', in: Denzin, N., Lincoln, Y., 2000, *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage Publications.

[95] *Ibid.*

[96] Miles, M., Huberman, M., 1994, *op cit*, p.265.

[97] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit*, p.93.

[98] Miles, M., Huberman, M., 1994, *op cit.*

[99] *Ibid*, pp.264-265.

[100] Eisenhardt, K.M., 1989, op cit.

[101] *Ibid.*

[102] *Ibid.*

[103] Hamel, J., Dufour, S., Fortin, D., 1994, *Case Study Methods*, USA: Sage Publications.

[104] Darke, P., Shanks, G., Broadbent, M., 1998, 'Successfully Completing Case Study Research: Combining Rigour, Relevance and Pragmatism', *Information Systems Journal*, 8, pp.273-289.

[105] Yin, R.K., 2003, *op cit*, p.47.

[106] Collis, J., Hussey, R., 2003, *op cit.*

[107] Gummesson, E., 2000, *Qualitative Methods in Management Research*, London: Sage Publications.

[108] Denzin, N., Lincoln, Y., 2003, *Collecting and Interpreting Qualitative Materials*, Thousand Oaks, CA: Sage Publications.

[109] *Ibid.*

[110] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[111] Selltiz, C., Wrightsman, L., Cook, S., 1976, *Research Methods in Social Relations*, (Third Edition), New York: Holt, Rinehart and Wilson, ASIN: B-0006-DADCQ, in: Gable, G., 1994, *op cit*, p.116.

[112] Which Popper has substantially devalued as an approach.

[113] Eisenhardt, K.M., 1989, *op cit*, 14, 4, pp.532-50.

[114] *Ibid*, p.538.

[115] *Ibid.*

[116] Popper's theory of 'critical rationalism' was itself a response to Hume's 'problem of induction', which essentially posits that, however much data one obtains in support of a theory, it is not possible to reach conclusive proof of the truth of that law. O'Hara (in 'Trust: From Socrates to Spin') argues that Hume's conundrum has still to be properly refuted. Nevertheless, how does science advance absent risk-taking and the proposition of new theories, which is of course precisely what this thesis attempts. Ironically, it was Popper, who purported the model of 'Open Society', which is germane to the broader, contextual aspect of this thesis; but was essentially inductive in approach.

[117] Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *op cit.*

[118] Eisenhardt, K.M., 1989, *op cit*, p.544.

[119] *Ibid*, p.545.

[120] *Ibid*, p.545.

[121] Private correspondence with Michael Herman, 16 August 2004; private correspondence with a PhD student at Brunel University conducting research into open source exploitation by comparing open with closed information prior to historic events.

[122] Interviews with SOCOM and OSJWG amongst others and treated further in Chapter Four.

[123] For example, the 1983 Franks Report notes the availability of open information prior to the Argentine invasion of the Falklands in March 1982.

[124] It is also worth remembering from Chapter Two that, where law enforcement is concerned, intelligence *qua* evidence is routinely required to be submitted in a court of law, where secret intelligence is not or cannot.

[125] O'Hara, K., 2004, *Trust: From Socrates to Spin*, Cambridge: Icon Books.

[126] Yin, R.K., 2003, *op cit*. pp.3-10..

[127] Scapens, R.W., 1990, 'Researching Management Accounting Practice: The Role of Case Study Methods', *British Accounting Review*, 22, pp.259-281; Otley, D., Berry, A., 1994, 'Case Study Research in Management Accounting and Control', *Management Accounting Research*, 5, pp.45-65; Yin, R.K., 2003, *op cit.*

[128] Eisenhardt, K.M., 1989, *op cit.*

[129] Interview, 2007, OSJWG 2, Cheltenham, 28 March 2007.

[130] Security is taken here to include all intelligence agencies. The author is cognisant of the differentiation between security as principally 'domestic' intelligence and intelligence as principally 'foreign policy' oriented. The author has observed in Chapter Two that this distinction is in any case becoming meaningless.

[131] The UK's Primary Joint Headquarters for example.

[132] Such an engagement is being actively encouraged. The open source environment is more suitable forum than the closed in this regard.

[133] Berkowitz, B.D., Goodman, A.E., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press.

[134] *Ibid*, p.41.

[135] The reason that organisations like In-Q-Tel in the US (openly funded by the CIA), and to a lesser degree QinetiQ/Dstl in the UK, have been established is precisely to encourage and financially support innovation in the private sector that may prove useful to the intelligence function.

[136] Confidential conversation with the director of a UK based PIB working for US agencies.

[137] There are two good reasons why OSINT should be observed against an all-source backdrop. First, closed sources can be useful for corroborating their integrity. Second, their effectiveness can be contrasted; not to determine, which is 'better' but how resource and expenditure might be more effectively allocated.

[138] Herman, M., 2001, *Intelligence Services in the Information Age*, London: Frank Cass; Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press.

[139] Collis, J., Hussey, R., 2003, *op cit.*

[140] Gummesson, E., 2000, *Qualitative Methods in Management Research*, London: Sage Publications.

[141] BBC Monitoring was formerly part of BBC World Service. The BBC is an organisationally and editorially independent public corporation.

[142] In April 2005, Her Majesty's Customs and Excise (HMCE) amalgamated with the Inland Revenue to form a new government department - HM Revenue and Customs (HMRC). This newer name is used throughout the thesis, but it should be understood that the organisation engaged with was known as HMCE at the time.

[143] For reasons to do with the nature of the 'target' that this organisation engages with, and as will be explained further in Chapter Four, this is not the real name of the organisation.

[144] It was publicly recognised for the first time in the Intelligence and Security Annual Report 2005-2006, 20 June 2006, report No: Cm 6864, p.8.

[145] Collis, J., Hussey, R., 2003, *op cit.*

[146] Eisenhardt, K.M., 1989, *op cit.*

[147] *Ibid*.

[148] For example, in the case of BBC Monitoring, it would be incorrect to say that senior executives were 'interviewed'. Rather, informal conversations were conducted throughout the research effort and the final summaries submitted for correction, clarification, and further discussion.

[149] For example, where open source exploitation was discussed under Chatham House rules by presenters to the Oxford Intelligence Group.

[150] Eisenhardt, K.M., 1989, *op cit.*

[151] Gill, P., Phythian, M., 2006, *op cit.*

[152] *Ibid*, pp.20-38.

CHAPTER FOUR

DERIVING THE HIGH ORDER FACTORS OF OSINT EXPLOITATION

> "Open-source information now dominates the universe of the intelligence analyst, and this is unlikely to change for the foreseeable future."
>
> John C. Gannon, 2000[1]

4.0 Introduction

In this chapter the author develops the model of high order factors that describe OSINT's specific contribution to the intelligence function. The data come from case-studies of organisations that exploit open sources for the intelligence community. Aside from describing contribution, the model might usefully be utilised across the intelligence function as a basis for understanding the effectiveness of open source exploitation if not its internal 'measurement'. The model is constructed iteratively, reflecting sequential phases of data capture during the research effort. This sequence of iteration also reflects an increasing depth of engagement with the case-studies, as well as an increasing confidence in the model's reliability.

Throughout the chapter the terms 'open source cell' and 'open source effort' are generically used to describe the particular open source structure within a particular case-study. Unsurprisingly in a research piece over such a time period (2002-2007) the personalities, titles, structures, resource, and, in one case, the very existence, of the respective open source efforts changed considerably. Nevertheless, it is the thrust of their endeavours that is of interest to the research.

The high order factors are derived through triangulating three sources of data:

- The claimed 'benefits' of OSINT exploitation found in the literature.
- Participant-observation by the author of OSINT exploiting organisations inside and outside the intelligence community.

- Semi-structured interviews with open source intelligence (OSINT) producers and customers within the intelligence community.

The chapter is divided into four parts:

- Part One - **preliminary findings**, which describes the initial research enquiries across a variety of intelligence and law enforcement organisations.
- Part Two - **model development**, which expands upon the preliminary enquiries looking at some organisations that specialise in open source exploitation, in particular the experience of private information brokers.
- Part Three - **model confirmation**, which demonstrates and effectively tests for the high order factors in one extensive case-study.
- Part Four - **other common features** of open source exploitation derived across all the case-studies.

4.1 Part One: Preliminary findings - beginning to examine the intelligence community

This section summarises the preliminary findings from the data collected against each of the case-studies detailed in Chapter Three (3.2.6), and coordinates them at the end. Not every case-study demonstrates every high order factor equally. Some interviewees express them with different words, but essentially say the same thing. Some of the factors are more significant than others because of that organisation's own particular objectives, processes, culture, or constraints. Indeed, in this phase the author was not sure which factors would emerge either to enhance or confirm the literature view. Thus the process is genuinely explorative and iterative towards construction of the final model.

4.1.1 DIS and EUROPOL: Setting-up, organising, and demonstrating effectiveness for open source exploitation

The DIS and EUROPOL were early pioneers of formal OSINT exploitation operations within closed intelligence and law enforcement agencies. Both cases illustrate well how OSINT exploitation was conceived and organised in a deliberate rather than ad-hoc sense. In particular they both demonstrate how to resolve the initial important challenge of demonstrating the perception of real benefit. Although serving different 'masters' their operations appear remarkably similar on the surface: the open source cell is centralised; small in terms of number of personnel; and they 'push' generic information to analysts on balance more than the analysts come to the cell to 'pull' more bespoke information from it.

In their early days, establishing an open source cell was met with some scepticism by the parent organisation. Like many new initiatives, it had to prove itself. By far the most important 'mark' for these new organisations was justifying their existence in resource and expenditure terms rather than in terms of outcome. Thus, the main benefit of establishing an OSINT cell became a cost-centred and administrative one, derived through the centralising of all open source collection. Rather than the Janes' or Lexis-Nexis' product being bought and paid for through single licence fees arranged individually by analysts, an organisation-wide contract established immediate economies of scale. The notion of purchasing once for the organisation, if not the community, was conceived in the face of commercial organisations selling many times to disparate intelligence organisations.

It is perhaps surprising to an outsider that such economies of scale are not transparently obvious. However, the inherent nature of compartmentalisation within intelligence communities both prevents such obvious collaborative activity and promotes a 'knowledge is power' approach that intelligence practitioners (collectors and analysts) can wittingly or unwittingly display. The OSINT cells themselves recognised that measuring their contribution in this way, quite apart from the obvious fact that cost savings would inevitably plateau and become meaningless, was not their 'be all and end all'. However, it

is important in the start-up phase to score an early hit with a parent organisation, which is perhaps as focussed (rightly or wrongly) on resource expended than outcome derived. This sense of 'acceptance' seems to represent the first tipping point moment for a newly established OSINT cell.

However, this momentum seems to be carried through and beyond mere acceptance to a further tipping point - 'indispensability'.Here, the customers of OSINT cells, the analysts, fall into a trap partly of their own making. They 'test' the new resource. Both these case-studies demonstrated some initial effort by the OSINT cell's customers to undertake their own OSINT exploitation, either by way of 'checking up' on the product delivered, or by way of competition to the cell's output. This practice by customers proves to be an opening for the open source cell that allows them to demonstrate more meaningful value. A self-realisation occurs. As the desk-officer analysts attempt to add to an already busy workload they recognise the additional and nugatory effort involved in matching the OSINT cell output. At the same time familiarity, trust, and satisfaction builds up amongst the customers to a point where the OSINT cell becomes the default first point of collection effort without question:

> "I used him (the open source cell) all the time as the first port of call."
>
> EUROPOL 6.[2]

Thus, the OSINT cell and the incorporation of open source product is routinised and institutionalised. It becomes effectively indispensable. However, this is where the two cases part company. At the time of the research, EUROPOL seemed to have managed this indispensable characteristic whereas DIS had clearly not. There seem to be two important features that might go some way to explain this: first, 'buy-in' at board level; second, a simple geographically disadvantageous location for the DIS cell. Whereas EUROPOL had the support of its Director (including by extension an invitation to the author for this research), the same could not always be said of the DIS for their open source cell. Furthermore, the DIS cell is inconveniently located, geographically and practically, in the basement of its Whitehall office, physically quite remote from the analysts, whereas the

EUROPOL effort, although outside the analysts secure area, was physically located centrally within EUROPOL itself. This quote from DIS ANON R1 is instructive with regard to location as well as 'push' versus 'pull' information procedures discussed later:

> "It's also a matter of geography. I try to stay in my office because everything I need is there. They are two floors away in the basement [referring to the Open Source Cell]. It's just too difficult to go there."
>
> DIS ANON R1[3]

This was subsequently confirmed by several DIS analysts who volunteered (un-requested) the same view during a presentation the author gave to the Cabinet Office Analysts Course in February 2007. Of course, geography and process are not the only explanations, nor are these the only two tipping points.

It is important to note that notwithstanding the provision of a discrete open source capability, open source exploitation by analysts continues outside the OSINT cell. This occurs: where it is considered necessary for security reasons; where it is felt that the analyst needs to have the information 'run through his own fingers' rather than the filter of the OSINT cell; where ignorance of or mistrust of the OSINT cell emerges; or a combination of these reasons. With the exception of mistrust, the dilemma of where to locate an open source effort - geographically, organisationally, and ideologically - appears to be a key universal conundrum for open source exploitation. It is not viewed as a sufficiently significant information source to be given distinct intelligence agency status, yet it is considered sufficiently useful that analysts will undertake it themselves. This raises questions of how best to allocate open source expertise - centrally to concentrate resource, dissipated to where it is required, or some combination of these.

In their effort to demonstrate the contribution of open source exploitation in terms of worth or value, both DIS and EUROPOL demonstrate three clearly discernible stages in the initial development of an OSINT capability:

- First, a proof of value in simple cost savings terms. This is more easily and initially achieved by an examination of cost benefits to the cell's broader organisational setting using a crude, but effective, before and after start-up comparison. The notion of utility is recognised.
- Second, a proof of value in terms of acceptance or trust. Here, there is a need to respond to the customer's needs. The OSINT cell can contribute in two clear ways: speed of response; and volume of information. Interviewee DIS ANON R1 demonstrates the customer's dilemma perfectly. This analyst, working in an all-source environment, made two points that are repeated across the case-studies. First, that open source information allows the interviewee to meet requirement deadlines that closed information sometimes cannot. Second, that open sources can actually contribute information with which to answer a requirement question, again where closed cannot. These are powerful capabilities that open source cells can demonstrate. The first reinforces a notion that in some way open source exploitation confers utility. The second remains more broad and vague at this stage.
- Third, a proof of value in terms of indispensability. As the notion of utility grows – cost, speed, and volume – so a base is created for beginning to display value in additional, possibly more meaningful, ways. This is almost invariably done by some informal (anecdotal) or formal measurement of customer feedback. For example, the fact that workload can be controlled is taken as positive indicator of value, or simply the volume of customer requests for open source exploitation is considered a useful measure. Most of the case-studies encountered have developed measurement systems ranging from a simple questionnaire[4], through deliberate interviews, to mandatory return-assessment-sheets attached to every OSINT product[5]. The return from these can be used to display to the parent organisation increasing sophistication and self-justification.

Throughout these three stages the perceived value of an OSINT cell to its parent organisation through the bestowed value from customers upon the OSINT cell increases rapidly. The author has not visited an OSINT capability that did not show these early

stages of mutual benefit. The broad value of OSINT exploitation is almost always appreciated. However, it is also clear in the early establishment of an open source effort that the value is derived partly as a result of its novelty and partly as a result of the attitude displayed by the cell members in their desire to succeed. There is also a clear satisfaction with the product as demonstrated by the customer but no formal mechanism to turn that into a measure of true intelligence effectiveness, if indeed such a holy grail exists. Equally, there is no 'halfway house' that demonstrates the specific contribution of effectiveness delivered by open sources alone.

Thus, the first clear benefit of OSINT exploitation begins to emerge from these two cases and is similarly evident across all the other cases - 'utility' - specifically cost, speed and volume of information supplied. Equally, these two cases chart the path that a start-up OSINT cell pursues, almost intuitively and generically, as they demonstrate cost benefits to gain acceptance and then indispensability before it can begin to demonstrate effectiveness. Finally, they demonstrate the conundrum of where best to place an open source capability - centrally, distributed, or a combination of the two.

4.1.2 BBC Monitoring and ICTY: To analyse or not to analyse?

> "Open source material derived from overseas media is rich resource, which can be mined at a low cost relative to the benefits it yields."[6]

BBC Monitoring is a curiously positioned organisation with regard to the UK intelligence community.[7] It is clearly not part of the Single Intelligence Account, nor is it a recognised intelligence agency like other members of the intelligence community beyond the SIA. Yet, it is a significant contributor to all of them. Furthermore, it is a contributor of information across UK government departments, to other national government departments, and many other international organisations inside and outside intelligence communities. It is not itself a government body; but sponsored by an amalgamation of UK government departments and agencies, now led and coordinated by the Cabinet Office, following a Cabinet Office-instituted comprehensive review of its operation and funding in 2004/2005.[8]

These stakeholders include: Cabinet Office; MOD; FCO; more recently the intelligence and security agencies; and the BBC Global News Division of which it is part. It has neither fully public nor private sector status, but resides somewhere in the middle. It is excused the profit motive, yet expected to begin 'paying its own way', with permission to supply to other sectors under certain restricted (security) conditions.

Along with the DNI's Open Source Center (OSC), it is one of the original and deliberately established open source collection organisations monitoring media communications around the world.[9] The Director of BBC Monitoring has stated that the aim of the organisation is to: "Faithfully reproduce the spoken word - in depth, sustained, with global coverage".[10] To this end, the organisation monitors approximately 3,000 radio, TV, press, news agency, and Internet sources, in 100-plus languages, across 150 countries, with just over 400 staff on an annual total budget (stakeholder funding plus commercial income) of approximately £28 million, of which £24.6 million comprises a ring-fenced grant from the Cabinet Office.[11] It is interesting to observe more recently that, notwithstanding the broad customer-base, BBC Monitoring's status and funding has been precarious.[12] In cash terms, between financial years 2001/2002 and 2007/2008, its stakeholder funding has varied between £20-22 million; yet in real terms it has declined in the same period from just over £17 million to under £15 million. In cash and real terms it was £18.5 million in 1993/1994.[13]

BBC Monitoring select and validate media sources, collect and process media data, and then package, produce and disseminate it to customers. They are universally used by UK and US intelligence organisations as a valuable source of raw information. Clearly, they cannot undertake analysis in the conventional all-source intelligence sense. Yet, they can and do explain the types and examples of media coverage to their customers, in order to demonstrate trends in coverage and the differences in coverage of different media organisations. Thus, while they faithfully reproduce and disseminate the spoken word as an underlying collection requirement, they additionally interpret what they collect and disseminate as part of a specialised and particular media-based analysis for their

customers.[14] Here one begins to see the emergence of another high order benefit of open source exploitation that is somewhat controversial - the ability of or potential for open source information to be 'analysed' in its own right.

Within BBC Monitoring, as formerly with FBIS and now the OSC, raw data and collated information flows through the fingertips of experts with linguistic skills, cultural familiarity, and research skills that the traditional intelligence community struggles to muster.[15] Furthermore, their experience of 'time on target' as the CIA puts it for their own analysts, is recognised as vital and to be encouraged.[16] Having said that, it is equally well observed that 'bias' and 'framing' are almost impossible to refrain from unless endowed with the constitution of a saint.[17] A desk officer at BBC Monitoring cannot but help bring experience to bear upon the selection, collation and processing stages of the intelligence cycle. Arguably, if they did not come with a frame of reference by which to make judgements upon the material they monitor, then they would probably be found deficient for BBC Monitoring work. Finally, with regard to analysis, it is apparent from several visits to BBC Monitoring that arguably, and notwithstanding their expert media analytical capabilities, considerable resource in a broader analytical role still lies untapped. The new Memorandum of Understanding established in April 2006 with its stakeholders may prove useful in reorienting response to more 'strategic' requirements.

A more explicit form of analysis is their monitoring of what is *not* said as much as what is. In this regard, for example, they were the first to note a tipping point in the 2004 Ukrainian election campaign, which they repeated later in Uzbekistan.[18] Similarly they were praised for making sense of the complex situation surrounding the Beslan siege in 2004.[19] Arguably, the short-list of 'firsts', but perhaps more importantly the provision of clarity behind the conventional media stories for decision-makers through 2006/2007, indicate that they are often better placed than closed sources to interpret crises *du jour*.[20] Indeed, it may be that open sources are the only resource in crisis situations (see endnote 85).

By contrast, the International Criminal Tribunal for the Former Republic of Yugoslavia (ICTY) demonstrates the ease with which open source lends itself to analysis simply because it is almost exclusively the only 'intelligence' input to what is a combined law enforcement and judicial process. Like many national intelligence capabilities beyond the US and UK, they have no choice but to exploit open sources of information because their recourse to closed collection methods is minimal. However, ultimately, they still regard their product as something that is passed on to other more final 'experts' or analysts; in this case prosecuting lawyers. Thus, it would be accurate to see the prosecuting lawyers as equivalent to policy-makers or decision makers within governments, who ultimately decide what to do with the final intelligence product.

ICTY conducts intelligence operations for evidential purposes. The data that forms this evidence is largely historical, largely print or broadcast-based, and intensely language specific. Hence, there is considerable open source effort. The ICTY is a good example of both OSINT cell informal analysis and customer open source research combined. Other than private sector operations, it is rare that OSINT cells are actively encouraged to analyse their own material albeit informally (the Asian Studies Detachment, considered later, is an exception). By the same token - resource constraint - its customers are actively encouraged to conduct their own open source research and exploitation. Only when the ICTY customers (prosecuting lawyers) cannot undertake their own research because of these added complications then the specific skills of the OSINT cell are tasked. Indeed, if it is felt that they (the lawyers) could conduct the research themselves then they are 'politely' invited to do so. This is an important point reflected in a 2006 Congressional Library Report, where it is noted that: "The availability of OSINT also raises questions regarding the need for intelligence agencies to undertake collection, analysis, and dissemination of information that could be directly obtained by user agencies."[21] In other words, put politely - do it themselves. It raises a further question on the precise location of open source exploitation and the desire for or against an independent open source capability.

The ICTY open source effort emerged informally to settle at an OSINT cell of only four or five strong. All these personnel have multi-linguistic and multi-cultural experience of the former Republic. Additionally, they have post-doctoral research skills and prior 'time-on-target' expertise that allows them to analyse the information as they collect and collate it, although they do not themselves see that what they do is analysis but just part of the total package they provide. Effectively, all phases of the intelligence cycle (absent requirements and feedback) are conducted within the ICTY open source cell. This ability to analyse reflects an emerging differentiator of some OSINT exploitation examples compared to others, namely that the OSINT cell members have an analytical capability by virtue of their language, culture, skills and experience. Interestingly, technological solutions for exploiting data are also initiated and delivered from within the open source cell. It is worth noting, as possible vindication of an open source exploitation system working for its customers, that the OSINT model was transferred to the International Criminal Court under the leadership of one of the founding members of the ICTY open source cell (Team Leader), with effect 2003.

Both ICTY and BBC Monitoring staff commonly display linguistic, cultural, and research experience, combined with tenure in post and time on-target; all the essential characteristics of an intelligence analyst not often achieved or supported as career options within some intelligence organisations, as Goss noted on taking over the CIA in 2004.[22] The author was of the impression that this was a bone of some contention in both organisations. Certainly, neither would categorise themselves as intelligence analysts *per se*. Yet, while, the ICTY open source effort would not claim to *formally* analyse the product of its collection, it does assess and interpret that collection effort so that its customers can better understand and gain insight from the product. Whether it has the time, inclination or sufficient resource is another matter. BBC Monitoring would go further and argue that they do undertake formal analysis of their collection effort and of a very particular and specialised nature pertinent to media sources. That they deliberately filter their collection effort, as in the case of ICTY, or that collection by BBC Monitoring is still predicated by the stated interests and priorities of their stakeholders, is incidental to the research question,

but crucial to a wider policy discussion on open source exploitation. These case-studies both demonstrate that open source has a potential for analysis in its own right and is similarly supported by the evidence from other case-studies notably the private information brokers and the ASD.

4.1.3 Her Majesty's Revenue and Customs (HMRC)

Access to HMRC was brief and limited. Notwithstanding the opportunity to speak with its then Head of Intelligence Analysis, who endeavoured to gain access for the author to engage with the Law Enforcement open source effort, only one interview with one desk officer at the open source site was possible. Further access was denied on the grounds that open and closed collection was difficult to separate out. The Head of Intelligence Analysis was based in London, while the Law Enforcement establishment, including the open source effort, was based in Ipswich. Nevertheless, some useful generic points were made from the two interviews, at very opposite ends of the hierarchy, that were reflected elsewhere.

The quality of information derived from open sources, in terms of its veracity, is determined partly by the sheer volume, the intuition of the human filter selecting it, and the expert judgement of the analyst utilising it. Essentially, HMRC use open source for horizon-scanning rather than 'point intelligence', for example likely economic impacts of threats to revenue in terms of VAT yield, rather than the time and place of a particular criminal event. Somewhat contrary to the reason for denying further access from the Law Enforcement unit, the Head of Analysis stated that open source exploitation creates its own discipline, but recognised that analysts have to use both open and closed sources together, which presents a security dilemma. Open source material is loosely classified at 'Restricted' level, but that does not necessarily alleviate sharing problems. As a consequence they operate a security policy of 'air-gaps' around computers and computer systems, which leaves many analysts unconnected to each other and rarely to the outside world.

The high order factor that HMRC seemed to support was the notion of providing context as being of value in its own right. Given the denial of access it seems only correct to place not too much emphasis upon this example as far as open source exploitation is concerned. The sense gained was that they simply did not want to engage with this research.

4.1.4 NHTCU and MPS

The law enforcement community's exploitation of open source is extremely disparate. It usually consists of two or three personnel working in other larger departments, which are seemingly oblivious to their existence. The level at which it is conducted is extremely junior in rank although extremely experienced in practice. Both the National High Tech Crime Unit and New Scotland Yard's (Metropolitan Police Service) open source units - two units with a clearly discernible open source capability - were run by Police Constables, albeit with many years service.[23] However, the contribution that open source is put to in this environment is the discovery of factual evidence; from the establishment of simple names and addresses to language translation. The emphasis of the open source effort unsurprisingly reflects the emphasis of law enforcement as a whole: an emphasis on gaining facts and evidence more so than understanding.

As was mentioned in the review of literature, there is a significant difference between law enforcement and security communities in terms of function and objective. The former's primary role is to uphold the law by pursuing suspected perpetrators of crime through the judicial system to the courts, based upon the provision of supporting evidence. The security and intelligence community's remit is not so specific. They have wider latitude, best summed up in the UK at least by the CONTEST programme – prevent, protect, pursue, and prepare – and their activity is based upon intelligence. Within the security community there is less need to emphasise the judicial route when an arguably more meaningful outcome is deemed desirable through detection, deterrence or disruption. While the law enforcement community tend to deal with the consequences of events, the intelligence community tend to deal with preventing events occurring at all. Of course these are fluid

boundaries and intelligence is practised within law enforcement as post event activity is conducted within intelligence and security organisations. Intelligence is not always evidence, but both exploit open source in pursuit of their objectives.

One of the anecdotal criticisms of open source exploitation is that it cannot reveal the 'who, when and where' of intelligence that traditional clandestine collection can. Apocryphally, it is said that such 'point intelligence' only ever occurs every ten years or so anyway. This notion of point intelligence is often erroneously conflated with interdiction or arrest when it might be more useful to talk about 'granularity' as the homing-in or focusing-in of information onto a risk event. In this regard, open source might be just as effective or ineffective as closed. The proof is ultimately revealed by outcome – arrest, deterrence, or detection for example.

In many cases open source cannot achieve what the traditional intelligence methods can when it comes to point specific or ground truth intelligence, sometimes referred to as the who, when, and where of intelligence.[24] OSINT tends to be more readily able to answer the how, why and who questions rather than the when and where questions. Historically this has certainly been the case whether by virtue of less competent technology, a less global society, different civil society attitudes favouring closure rather than disclosure of information, or a combination of all of these. As discussed in the literature survey, these changing factors and many other impacting factors are pressing to modify the balance.

This traditional model reflects contemporary assessment that OSINT contributes where coarse granularity is required. It provides broad context for 'sense-making' and/or 'quick and dirty' knowledge when events present themselves suddenly, while a more traditional closed intelligence aims for sharper granularity or more specific intelligence. However, this research's engagement with the intelligence community and open source practitioners suggests that this balance is changing. Open source can lend insight where fine granularity is required into a variety of contemporary challenges.[25]

Granularity is akin to a radio's 'fine tune' dial. However, it is not simply about the provision of detail. When there is no closed intelligence collection resource then open sources can be used to reveal something about a target or requirement that might trigger or direct other closed assets for tasking. This notion of 'focus' as both useful detail in its own right as well as trigger for other collection efforts is similarly demonstrated across all the case-studies. Equally, the notion that in the absence of closed information, open sources could rapidly and effectively 'surge' to build a picture against requirement was also apparent from the NHTCU experience in particular.

Thus, while the law enforcement case-studies display little about the generic organisational development of open source exploitation *per se*, they did reflect two important benefits of open source displayed across all the case-studies - focus and surge.

4.1.5 BBC Monitoring and US Special Operations Command (US SOCOM): The customer is king and the beginning of clear objectives for OSINT exploitation.

As section 4.1.2 explained, BBC Monitoring remains an intriguing case because it straddles several categories of institution. It is clearly a key contributor to the national intelligence output, though not a fully incorporated member. It has neither the status of intelligence agency like GCHQ, the Secret Intelligence Service (SIS), or the British Security Service (BSS) nor is it fully unleashed to make a profit like *Janes* or *The Economist Intelligence Unit*, themselves key contributors to open source exploitation. It is expected to provide the 'gold standard' service to its stakeholders, yet somewhat restricted from providing the same 'full' product to commercial customers. However, and regardless of this slightly ambiguous existence, it clearly understands that what its customers think of its product is critical to its survival. Furthermore, since 1939, it has recognised and exploited an important global open information source - broadcast media - in conjunction with its long time partner the former US Foreign Broadcast Information Service (FBIS) and now Open Source Center (OSC).[26] Today, both BBC(M) and the OSC handle all forms of media (not

just broadcast), including traditional and new forms.[27] To this end BBC Monitoring has regularly questioned its customers for feedback on its product.[28]

US Special Operations Command (US SOCOM) is one of two dedicated OSINT cells within the US Armed Forces established at Combatant Command. It is regarded by some as the pioneer of OSINT exploitation within the US DOD. It is supported at the highest levels, notably by the recently created Under Secretary of State for Defense Intelligence (Dr Stephen Cambone).[29] In 2005, commensurate with their role as lead military organisation in the 'War on Terror',[30] they established a dedicated intelligence organisation to GWOT, which incorporated the pre-existing open source exploitation effort.

In 2002-3, SOCOM's open source cell decided that justification for their effort could only emerge if their product was in some way demonstrable and measurable. Like many other open source efforts, including BBC Monitoring, they realised that their customers were best placed to assess the value of their product. They established a compulsory 'return view' or assessment for every item of product they sent out. However, they went one step further than other open source evaluation returns in that they asked their customers to evaluate open source in comparison to other closed sources. They quickly learnt that the OSINT contribution to the overall intelligence output was consistently perceived 'more useful' than other inputs. When these returns were correlated against relative established resource and budget it was simple to demonstrate comparative efficacy.[31] Not only did this place them 'on the map' within their much larger intelligence and operations organisation; but it also became a benchmark against which other 'ints' could measure themselves in terms of effectiveness rather than simply efficiency. Of course, unlike single source agencies, SOCOM is an all-source intelligence organisation and thus has more sources to compare against than a single source agency has.

Whether the customer ought to be the final arbiter of intelligence effectiveness is discussed further in Chapter Five.[32] Across society one might begin to question whether intelligence effectiveness should be assessed in terms of mechanistic target and league measures rather

than a more ontological sense of security. However, within the boundaries of the intelligence community, satisfying policy and decision makers is absolutely implicit in the definition of intelligence.

4.1.6 All Preliminary case-studies: 'Context' and 'communicability'

Without exception across the case-studies it was found implicit that open source is used primarily to provide context to a security or law enforcement issue. Arguably, context was the principle rationale for open source exploitation. In EUROPOL for example, analysts generally began their assessments with a request to their open source team for background information. In SOCOM this has become a formally accepted practice. In DIS, the open source team may not be the first port of call; but open source information is something their analysts normally turn to first. In a paper presented by the Director of the UK's Conflict Studies Research Centre to the CIA, three key contributing benefits were attributed to open source exploitation: "getting a basic grounding; sniffing the wind; and seeing what's not there, what others would like to hide …".[33] These might be interpreted as context, 'first alert', and benchmarking or checking respectively. However, there is a caveat here, which is discussed further in Chapter Five; not all 'targets' lend themselves equally to open source exploitation, and certainly do not always reflect the 80 percent rule often cited and aired throughout the literature.[34]

In a different way it is becoming increasingly explicit that open source can be used to communicate within and between intelligence agencies as well as beyond the intelligence community. Indeed, in the US, while it may be slow in happening, sharing is now mandated by Presidential Directive.[35] There are a variety of reasons why open source can contribute here. First, the sharing between agencies that has hitherto been frustrated by compartmentalisation and security issues, is eased by the universally lower classification attached to open source exploitation. Second, closed information can be 'masked' or 'covered' by the emergence of open; something discovered clandestinely can be actively sought openly in order to promulgate the essence of the closed information to a wider

audience. Interestingly, this of course represents a reverse in the flow of the *focus* benefit described above, as well as lends credence to some agency claims that they increasingly find it difficult to separate out closed from open.[36] Third, in an era of multi-national cooperation exemplified by structures such as CENTCOM or the Joint European Situation Centre (SitCen), where once trusted bi-lateral arrangements facilitated the exchange of closed information, the advent of open source exploitation facilitates a multi-lateral cooperation that closed information can not, but the contemporary context demands.

However, even with the formation of organisations such as the UK Joint Terrorism Analysis Centre (JTAC) and the Serious Organised Crime Agency (SOCA) - organisations created to cooperate across intelligence boundaries - the tendency is for new organisations like these to form new protective barriers and bureaucracies of their own. The US Department of Homeland Security is a similar example. The natural tendency to compartmentalise in preference to collaborate remains ascendant in the intelligence environment. The motives for doing so are more human and political although they are rationalised and expressed as security concerns. The US Select Committee on Intelligence reported the following in May 2004[37]:

> "Although efforts have been made to surmount restrictions, some information sharing limitations have reemerged in the very programs that were designed to address them. The operations of the Terrorist Threat Integration Center (TTIC) are a prime example of this transfer of limitations," the report observed.

On the other hand it may be that information sharing initiatives such as SCOPE in the UK and Intelink-U in the US might alleviate much of the security inspired resistance to collaborate; but the cultural proclivity to collaborate will likely remain an attitudinal one.[38]

This cultural resistance seems a worthy research topic in its own right. It certainly seems to be an important factor in understanding the role of open source exploitation in the broader intelligence effort. The cultural proclivity to closed information remains a stumbling block across all the case-studies observed. However, this cultural resistance to

OSINT is easing. Contrast the two anonymous DIS analysts. ANON R1 says that nearly all of his/her work is based upon open source material:

> "… nearly 100%.".

Why? ANON R1 states that there is very little between 'open' and 'STRAP' (Secret level intelligence from special sources) to allow the analyst to create output that is useable and timely for customers:

> "If I wait for stuff to be returned in a diplomatic bag, I will miss my deadline. So, I make do with other means. I feel like a journalist rather than an analyst."[39]

By contrast ANON R2 is critical of open source, at least critical of open source exploitation within the DIS, but states finally, if ambiguously, that:

> "… unless it is secret it is worthless."[40]

There is a growing realisation that knowing only secrets in our contemporary society hardly empowers a government to contribute to its electorate's perception and management of risk. As Steele remarks on his web site and in his literature: "Spies only know secrets"; and: "Do not send a spy where a schoolboy can go".[41] One suspects that this resistance may simply turn out to be a largely generational feature analogous to the debate over women membership of golf clubs.

4.1.7 Other contributing factors: Serendipity and horizon-scanning

Two further potential factors - 'serendipity' and 'horizon-scanning' - suggested themselves to the author during the course of these preliminary data collection efforts. Horizon-scanning because it had already featured in the literature, and serendipity because the author's own experience suggests that it features heavily in intelligence matters.[42] Serendipity - 'tripping over' things is a much maligned and unwisely satirised intelligence

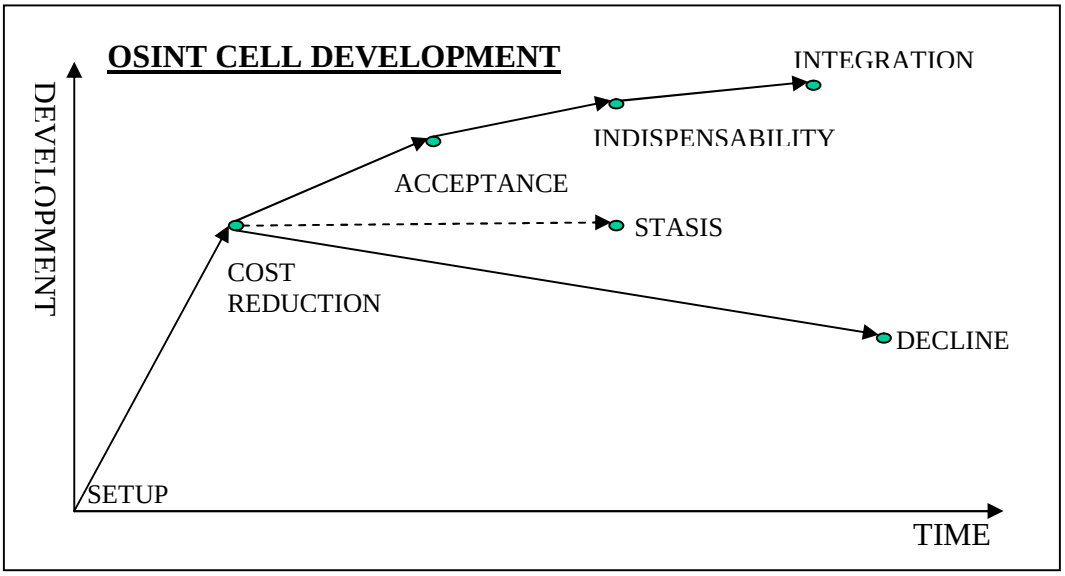
skill that with practice and experience can be connoted with intuition and gut-feeling.[43] Horizon-scanning is very much 'in vogue', yet difficult to entirely distinguish from what is broadly meant by understanding context. However, horizon-scanning has connotations of risk management and the 'what-if' of decision-making about it. Like 'groupthink', 'resilience', 'joining the dots', and 'failure of imagination', these terms become internalised and institutionalised without questioning their meaning. The pitfalls of this approach are treated in Chapter Five. Understanding context is based more upon political science and a 'what-**is**' approach to decision making. Arguably, these clichés can be more troublesome than useful. One might legitimately argue that the role of the intelligence community is to know what is beyond the horizon rather than what is on it. Perhaps the analogy of 'putting things on the radar screen', which by implication had not been visible hitherto, is more useful. A more pertinent question might be - how do the originators of requirements and their policy masters know what to ask for in the first place if they are not in some way scanning metaphorical radar screens. However, neither serendipity nor horizon-scanning featured in the research, and anyway are not necessarily exclusive to open source exploitation. Arguably, in the end, they are not so easily distinguishable from each other. However, they are highlighted here in preparation of subsequent case-studies.

4.1.8 Summary: OSINT High Order Factors and OSINT Development

Two key themes emerge from the preliminary case-studies: first, a sense that open source exploitation efforts follow a similar development route with key hurdles to pass in order to progress, and second, a notion that several high order benefits accrue to the broader intelligence function by virtue of pursuing open source exploitation.

The progression of an OSINT effort from genesis to integration is not the key theme of this thesis, but certainly part of its context. A representation of the broad development of an OSINT exploitation effort is summarised in Figure 4.1 below.

Figure 4.1: OSINT cell development



Source: Author

In addition to observing key contributing benefits of OSINT exploitation and the developmental path of an OSINT effort, the structure, process and environment of OSINT exploitation was also observed. These are discussed further in Chapter Five: how best to organise, where to organise, collection versus analysis, and some pitfalls.

More importantly, the review of literature indicated that the descriptors or high order factors common to the purpose of open source exploitation might include: matrix; surge; revelation; utility; and horizon-scanning. The preliminary research begins to suggest that these factors might more accurately be stated as: utility; analysis; context; 'first alert'; benchmark; focus; surge; and communicability. These high order factors are now developed further in the subsequent data collection.

The brief glimpses into how the author was 'handled' are included by way of illuminating how intelligence organisations themselves are responding to the post-Cold War environment, specifically the direction offered by post-9/1l and post-Iraqi WMD inquiries. It also recognises how they are coming to terms with the contemporary era of transnational threats and globalisation, where they could not rationally be expected to have all the

answers alone. To some extent it also illustrates the degree of confidence they have in displaying their efforts for scrutiny in sensitive environments, as well as the dilemma of revealing their intrinsic competence in a broader context that professes an openness and transparency of government machinery. This would be as equally true of an ethnographic research effort into commercial organisations for similar reasons of sensitivities.

4.2 Part Two: Model development - Private Information Brokers (PIBs), DIS and EUROPOL postscripts, and the UK Open Source Joint Working Group (OSJWG)

> "I have learned, however, from long experience in intelligence work, that much can be learned from open sources."
>
> Arthur S Hulnick, 2004[44]

4.2.1 Introduction

The next iteration of the research principally involved detailed study of three commercial private information brokerages (PIBs), a re-visit to the DIS and EUROPOL open source efforts, and engagement with the UK's Open Source Joint Working Group (OSJWG). This part of the research attempted to look at open source exploitation in the private sector including its relationship with the public sector. Organisations like Janes, the Economist Intelligence Unit, Oxford Analytica, and Factiva are 'household names' to the public sector intelligence community. They represent a staple diet and resource for most of their open source efforts. The three PIBs examined here are much smaller and specialised than their 'household name' equivalents. Hazard Management Solutions (HMS) collect and analyse technical intelligence on Improvised Explosive Devices (IEDs), Political Risk Associates (PRA) produces intelligence on single issue protest and pressure groups notably animal rights protest, and Exclusive Analysis (EA) on geo-political risk, notably the risk of violence and legal/financial risk. HMS has an extensive US government and smaller UK government clientele, PRA has a UK law enforcement and private sector clientele, EA has a private sector multi-national corporation clientele. They all enjoy niche reputations, yet

their subject matter is invariably global. They have all afforded the author virtually unlimited access to their operation. HMS has supplied the author on a monthly basis with five years worth of open source data collection and special reports, PRA has frequently supplied the author with product, and EA has supplied the author with its annual Political Risk Forecast.

These organisations exist because they are commercially viable. They are commercially viable because they supply a product that fills a perceived need by their customers. They exist because their customers say so:

> "(However), the mere fact that this business has grown over the past 15 years suggests that the rigorous application of open source intelligence gathering can deliver a valuable service—and one which companies are prepared to pay for. This service is underpinned, however, by a simple truth: if they fail to deliver accurate and timely intelligence then they will no longer have contracts with their clients. So what one has seen is the development within the private sector of the evolution of rigorous techniques, which provide companies with a valuable service."
>
> PIB 1[45]

Thus, it is instructive to understand precisely what is represented in this product that they supply to their customers and whether this contribution matches the claimed benefits of the preliminary findings. The author was granted unlimited access to and continuous contact with these three PIBs. It is worth noting that this part of the research was also punctuated by continued dialogue with the already-visited open source intelligence efforts, and an engagement with the UK Government lead elements of open source exploitation, notably the 'Open Source Champion' for the Cabinet Office, a representative from the Cabinet Office working with the UK's Joint Intelligence Committee (JIC), and the UK OSJWG.

4.2.2 Hazard Management Solutions (HMS): The 'one-stop' shop - collection to analysis.

Hazard Management Solutions (HMS) was established in late 2000 as a one-man band

operating out of the front room of a private house. By 2005, it employed over 40 people with offices in the UK and Washington as well as representatives in Iraq and Afghanistan.[46] In 2006, it had annual revenue valued at £6.6M with contracts to support defensive IED operations for several countries, including the US DOD, and multinational organisations, including NATO. In 2007 it was bought by Allen-Vanguard for $40M (Canadian).[47] HMS specialises in collecting and analysing data and information on a single global phenomenon - Improvised Explosive Devices (IEDs). It collates this information from openly reported sources and disseminates the assessment via a monthly summary known as 'TRITON' or via 'Quick Look' reports on significant incidents of note.

The managing director of HMS specifically defines OSINT as the product of 'visibility' and 'acuity'. It is difficult to conceal the incident of an improvised explosive device from the media. As a result of the open reporting of such occurrences, principally in print and broadcast media, they have 'visibility' of their target or subject matter. Of course it is not practical or economical for a business to purchase hard copy of every newspaper from Russia's *Pravda* to Karachi's *Dawn.* However, 'news aggregators' such as Lexis Nexis, Factiva and Dialogue, news agency 'wire' feeds such as Reuters and Agence France Presse, and BBC Monitoring or FBIS as was, can collectively pump digital copy to any PC with a telephone connection. PIBs are extremely well resourced to capture and process this data. They focus that data through the prism of their own experience – 'acuity' - interpreting what they see in a classic analytical way into knowledge or intelligence in order to support others who are engaged in policy and decision making for action. The author interprets this as simply the ability to conduct authentic analysis on the basis of experience applied to information.

The value of the open source technical intelligence they produce remains in the purview of the customer, notwithstanding the conundrum of how to measure intelligence contribution. Unsurprisingly, HMS customers include public sector 'counterparts' engaged in technical intelligence such as UK's Scotland Yard, DIS, and other intelligence agencies, plus the US's FBI, DOD and other intelligence agencies, together with several private sector

companies. Representatives of these organisations are in regular contact with HMS. Commercial contracts have been established with these organisations, and representatives of HMS regularly communicate with them. In the absence of an equivalent capacity, HMS seems to provide something that these organisations consider useful. Essentially they fill a gap, which the public sector organisations cannot accomplish within their own resource. In the US case, largely because of an absence of any significant homeland terrorist activity, they have leant heavily upon, and learned quickly from, the UK's specific Northern Ireland experience, which they have applied both at home and specifically in Iraq and Afghanistan. In the UK case it adds additional interpretation into an all-source effort - analysis - as well as sensible utilisation of societal resource. This might be interpreted as a surge effect in the US case and simple utilitarian common sense in the UK case.

Interestingly, two additional features are observed. First, in HMS' case alone, some of their customers have discussed the practicalities of reversing out closed sources of information from their intelligence activity into HMS activity in order to produce a fuller assessment. It is difficult to know whether it has actually happened given the confidentiality concerns of the company and the security concerns of the intelligence organisations. Thus, it was not possible for the author to verify the authenticity of this statement. However, there is no doubt that it has been seriously discussed. That it is mooted at all is interesting. Second, the evidence from HMS, and supported by PRA, suggests that, because of their experience, the creation of intelligence is also being supplemented with direction to decision-makers on action. Security, law enforcement, and private companies alike seek advice from these PIBs on how to act. The distinction between intelligence, policy, and action is more mixed and blurred than might be expected. It is almost as though the bureaucratic restrictions that exist within public sector hierarchies are less apparent when dealing across sectors, perhaps refreshingly so. Common professional expertise, indeed common personal experiences in many cases, create comfortable working arrangements for common benefit. The sharing of information and the professional regard for its assessment are mutually beneficial. However, the ability to distribute information gleaned by open sources down to the point on the ground where it

might achieve maximum benefit may very well be life-saving. The ability to communicate this information where closed collection prohibits it is a significant contribution.

However unsatisfactory it may seem, the reactions and responses of customers to the services provided by PIBs seem to be key 'measures' of success. In the private sector, varying ways of estimating how such information contributes to the 'bottom line' are made. However crude or sophisticated they appear their aim is to gauge how such information has helped commercial corporations to achieve objectives that they set themselves. The bottom line is of course less pertinent to the public sector. Here the contribution of PIBs, by implication open source exploitation, is to:

- Fill both capability and capacity gaps, thus providing information and analysis more cheaply, more quickly, and in greater depth of coverage than could otherwise be achieved by their own resource.
- Communicate otherwise classified information.
- Surge information to rapidly fill information and experience gaps.
- Provide interpretation of data that either stands as analysis in its own right or contributes further to all-source analysis.

Temptingly, since HMS now has seven years of data and analysis on the global incidence of IEDs, it would be interesting to contrast the relative understanding of technical intelligence held openly against that held by closed organisations in order to determine the best relative allocation of resources.

4.2.3 Exclusive Analysis (EA): Good enough strategic assessment

Exclusive Analysis is a medium-sized company that, like HMS, emerged in late 2000 offering 'bespoke', geo-political analysis. It specialises in forecasting political risk and violence worldwide. Like HMS, EA was started by one person with a relevant intelligence and security background and a single commercially viable idea. Today EA is located in

the City of London employing approximately 35-40 staff with a predominantly multi-national corporation (MNC) clientele. The two striking features that are immediately apparent upon walking into EA is that it is a relatively young organisation (mid-20s to mid-30s) and that it is multi-national, that is to say linguistically and culturally diverse. EA is by no means unique in these respects within the private sector, nor is what they do. There are many bespoke geo-political risk companies, some of them, like Control Risks, have become multi-national entities in their own right. Furthermore there are numerous strategic think tanks, which cover very similar territory. However, with the exception of BBC Monitoring and the Asia Studies Detachment no such similar cultural and linguistic diversity was observed within an open source effort serving the public sector. In some cases, of course, it is simply not necessary, as the next case-study demonstrates. Nor is it to say that such expertise does not exist, but it certainly was not as immediately apparent as EA.

EA presented an opportunity to explore, albeit cursorily, whether they really could reflect the trappings of an intelligence function in terms of forecasting likely future events and scenarios from purely open source means. In December 2004, Exclusive Analysis published their 'Global Risk Outlook' report for 2005.[48] The 'intelligence cut-off date' was set at 1st December 2004. The report makes a variety of forecasts on political risk and the likelihood of violence for 2005. Three examples are detailed below.

- <u>An attack on UK mainland in 2005</u>

> "From 2002, we were fairly confident that there would be no major successful follow up terrorist attack in the US or UK. We held this view until April 2004, when certain factors persuaded us that an attack had become more likely by the end of 2005."[49]

This claim is repeated and supported throughout the report.[50] It is based upon their observation of evidence in the public domain such as the interception of 'green shoot' Sunni extremist movements by intelligence and security agencies, the arrest of

individuals and small groups with bomb-making equipment intending to make attacks, and evidence of cooperation between existing terrorist organisations and Sunni extremists as in Madrid. Finally, the report states:

> "We now hold, and after bin Laden's appearance [October 2004], maintain, there will be an attack before the summer of 2005, albeit on a more modest scale than 9/11."[51]

Not only are they forecasting a 'cut-off' date, but they also forecast an upper impact range. Again this latter point is backed up by an analysis of previous incidents that display a significant element of human agency, but excluding natural disaster.[52]

Between March and November 2004, various establishment 'heads' including Sir John Stevens (Metropolitan Police Commissioner), Dame Elisa Manningham-Buller (Director-General Security Service), and Ken Livingstone (Mayor of London) warned of an "inevitable", "imminent", and a "not if but when"-attack on the UK.[53] The Joint Terrorism Analysis Centre stated after bin Laden's appearance in October 2004 that the threat to the UK was real and serious, and likely to persist.[54]

One could argue *ad absurdum* and without much satisfaction as to who forecast the July London bombings first. Furthermore, does it matter? Equally, a private information brokerage established in 2000 has a long way to go before it can claim a track record in forecasting compared to the traditional intelligence community with decades and generations of experience. Perhaps, more importantly, one could argue that they did not satisfactorily explain why the London 2005 attacks occurred at all.

More significantly, for this research, two points stand out. First, that a private information brokerage forecast it at all. Second, that unlike any other organisation, they forecast a date with an impact.[55] To the customers of EA, one might tentatively suggest that this forecast displays some of the high order contributing factors identified in this chapter, notably: 'utility' in terms of cost, 'communicability' in that it is useable

material, ‘analysis’ in that it is evidence-based, ‘focus’ in that it creates granularity, and ‘benchmark’ in that they can compare to their own or external information sources. It is difficult to suggest that the forecast represents ‘context’, although the report in which the forecast is made certainly does. Furthermore, for customers of EA they will have access to the model, algorithm and supporting data as context. It is also difficult to argue ‘surge’ as this is a main focus for EA anyway.

- US foreign policy towards Syria in 2005

> “All of these developments [in the ‘War on Terror] will take place against a background of what few in Europe think possible – a more aggressive US foreign and security policy. Syria, Iran and North Korea will attract Washington’s attention. But as the softest target, Syria is probably most vulnerable.”[56]

Again, the forecast is supported with evidence throughout the report.[57] It is much less ‘focused’, as in granularity, than the item above, in the sense of when, where, who, and how much. Rather, it is much more contextually nuanced - having to rule out alternative options before alighting upon the last one standing.[58]

A US military incursion into Iran is ruled out as being too much to undertake while Iraq remains insecure. The potential nuclear weapons threat, particularly to Israel, emerging from the Russian-backed nuclear energy programme is noted; but still within the realms of non-violent or ‘soft-power’ solutions led by the EU. Furthermore, much of it is widely dispersed and underground. Thus Syria becomes the US target of attention by dint of weakness - economically, politically, and geographically. It is economically and militarily weaker than Iran. It has no potential or discernible nuclear arsenal, but some limited WMD programme. It is geographically sensitive in that it borders Israel with whom it has not concluded peace negotiations, and Iraq across whose border it ‘trades’ insurgents.[59]

The EA report was published before the death of former Lebanese Prime Minister Rafic Hariri on 14 February 2005. Hariri's death ushered in the withdrawal of Syrian forces from the Lebanon by May 2005. Senior Syrian establishment figures were implicated in a UN sponsored report published in October 2005.[60] The US, led by Condoleezza Rice (US Secretary of State), then initiated political pressure upon the Syrian regime, supported by Jack Straw (UK Secretary of State for Foreign Affairs) in calling for 'something to be done'. What that 'something' was did not emerge in 2005, which the EA report also noted. Furthermore, and pertinent to why that something was difficult to articulate, the EA report went on to note that: Israel would rather have a stable secular government for its neighbour than the alternative - Islamist chaos; the US recognised Syria's intelligence services as being valuable asset(s) in the 'War on Terror'.[61]

The EA report did not specifically forecast the assassination of Hariri or the subsequent implication of Syria, which presented the US with an opportunity to increase political pressure; but it certainly displayed the high order factor 'context', as in the general thrust of US foreign policy towards Syria, based upon its analysis. It goes on to add 'focus', when it suggests that attacks against Israel by the Lebanese-based, Syrian-backed Hezbollah movement would be blamed more upon Syria than Lebanon.[62] The report suggests that this in turn might precipitate an alternative US security option. However, while this did not emerge in 2005, the Israeli invasion of southern Lebanon against Hezbollah positions in July 2006 might be interpreted as that US-Syrian engagement, albeit by proxy.

- <u>Saudi succession scenarios in 2005</u>

> "We do not support the general view that there are risk-laden succession scenarios within the House of Saud. … Although all the ingredients for a turbulent, and potentially violent, power struggle may be present, the Saudis have managed complex succession processes in the past, and it is highly unlikely that [Crown Prince] Abdullah will be prevented from ascending to the throne."[63]

King Fahd's death was announced on 1st August 2005. He was seamlessly replaced by the de-facto ruling Crown Prince Abdullah, who was invested on the 3rd August 2005.[64] This forecast displays both focus and context, again with supporting evidence.[65]

The context describes the historical emergence of the Kingdom of Saudi-Arabia under Abdul Aziz al-Saud between 1902-1932, and the tentacle-like nature of the House of Saud that consolidated its hold on the kingdom throughout the 20th Century. The EA report refers to the 'Sudairi Seven' – King Fahd and his six full brothers – who constitute the Abdul-Aziz faction of the Royal court, together with the Crown Prince's counterweight found in the al-Faisal branch of the family. The report points out that Abdullah is less inflamingly opulent than Fahd. He is difficult to pinpoint as either conservative or liberal. He speaks little English. He does not holiday in the West. He is pious. He is pan-Arabic. He has cut royal stipends and curbed royal abuses. Above all else he understands that Saudi-Arabia must develop an institutionalised representative government. The chaos that would emanate from a failure of regime survival unites the entire family. The particular obstacle to modest liberalisation - Prince Nayef, the Minister of the Interior - is highlighted. However:

> "The lack of wider popularity makes a visible power struggle dangerous for the House of Saud. … The current struggle is more one of individual posturing for the sake of an enhanced self-image, than a genuine threat to the established order."[66]

The focus is to be found not just in correctly identifying that Abdullah would succeed unopposed and with ease. Rather, the focus is to be found in the timing of the report – the fact that it was raised as a subject at all. This is what intelligence professionals would call 'timely'. Arguably, predicting that an ailing person is about to die seems little challenge. However, this person, in the troubled regionally insecure Middle-East, in the midst of difficult if not deteriorating national internal security, with external pressures being loaded on by the US,[67] and with a war on its border, seems a very 'useful call' to customers who have commercial objectives to fulfil.

This is highly communicable or useable information. Furthermore, it begins to demonstrate the added value that intelligence can bring to decision making and risk management. Risk management is about managing uncertainties in order to maximise the achievement of objectives.[68] Inevitably this involves decision-making, which in turn necessitates information upon which to make decisions. The better the information, all other things being equal, the better the decision. Any company with commercial interests in Saudi-Arabia may have been thinking about their future in the kingdom in late 2004. The internal security situation of 2003/4 was already tense.[69] A disputed succession and consequent fall-out may have tipped the balance. An authoritative report such as this may have been welcome.

4.2.4 Political Risk Associates (PRA): Open or closed?

It is necessary to state at the outset that Political Risk Associates is not the real name of this organisation. For obvious reasons the name of the company and the individuals concerned are deliberately withheld, given the irrational and immoderate activity of the object of their collection effort. PRA is essentially a one-man band and has remained so since its creation in the late 1980s. Again it was the invention of one person with an interest (a curious interest) in the activities of single-issue protest and pressure groups, principally the activities of 'animal rights' activists. The individual was able to commercialise the product for the benefit of law enforcement and private sector commercial organisations.

Activist groups have targeted UK commercial organisations for over 15 years. During this period they caused financial damage and disruption to legitimate business activity, including by way of example:

- An ongoing animal rights campaign against Huntingdon Life Sciences that has so far persuaded 358 other companies to sever their links with the animal-testing laboratory.
- An 'anti-roads' protests in the 1990s that stopped the then Conservative Government's road-building programme. Tarmac's additional security costs for the M65 construction

programme amounted to £450,000 per month. It failed to stop disruptive protest and arson attacks.

- 'Anti-GM' activism targeted Monsanto in opposition to the development of genetically-modified crops in the UK. Despite the use of lawyers and PR professionals, the campaign succeeded in Monsanto's withdrawal from GM testing in the UK.

It is worth mentioning that even in the very specific arena of animal rights activism, there are several such bespoke organisations collecting against animal rights activists. Charitable organisations, NGOs, the UK police National Extremism Tactical Coordination Unit (NETCU), the UK police National Public Order Intelligence Unit (NPOIU), the UK Police National Crime Squad, and MNCs with their own in-house capability, are all engaged in 'monitoring' the debate over animal experimentation versus animal rights and its potential implications. Arguably, in these and similar risk debates, the one thing that does not happen is a full and open public discussion about the issues. The gulf between the perception and the reality of the risk in this and other forms of extremist activity can be a paralysing one. For the purposes of this research the author is not interested in the debate *per se*. Rather, the research is solely interested in the exploitation of open sources of information that contribute to the law enforcement and commercial side of the debate.

From the commercial point of view it is not simply personal injury and damage to personal property that exercises them, but also the protection of reputation that influences share price, cash flow, turnover, and debt levels - all key significant economic indicators. Because of this reputational risk migrating to significant economic risk, it is politically convenient for targeted companies to monitor that risk at one remove rather than be seen to actively conduct information-gathering endeavours themselves. Typically, MNCs will pay between £2-12,000 monthly for such service. In a sense this is communicating or 'covering' closed or sensitive information via open means.

There are reckoned to be some 4,500 activist groups in the UK alone. It is simply beyond the existing capacity of public sector agencies or private sector corporations to monitor

them in the way that bespoke organisations such as PRA can do. Furthermore, because of the flexible and erratic nature of many of these protest groups they switch targets rapidly and often. Mirroring the variety and agility of these organisations is difficult to initiate from within somewhat bureaucratic and otherwise engaged organisations. They are more easily matched by surge efforts from those who can:

> "It is often necessary to respond quickly to a new threat and is far easier for companies to seek specialised outside advice rather than attempting to develop an in-house capability."
>
> PIB 1[70]

PRA is careful to mention that how they exploit open source information is not significantly different to the methods adopted by public sector organisations. Interestingly, they both additionally employ limited alternative sensitive means to gather information, and in PRA's case it is difficult to know where open stops and closed begins. The author was not made privy to the sensitive means and so cannot verify them, but, like HMS and the reversing-out of sensitive information from its clients to HMS, there is an element of all-source information gathering going on. Several advantages are claimed over the public sector effort:

- PRA is only focused on what the client needs to know.
- The police are constrained by resource, competing requirements, the bureaucracy of public sector organisation, and the 'competition' between interested agencies.
- PRA is quicker to report to clients than public sector organisations. This is partly because it is their commercial interest to do so, and partly because they are unhampered by intelligence classification.
- PRA can give a focused assessment that corresponds to a realistic approach to risk rather than a precautionary principle approach. That is to say they produce a 'most-likely' rather than 'worst-case' assessment. This is treated further in Chapter Five within the analysis on the pitfalls of an inappropriate risk-based approach.

- PRA has far greater amounts of information available on what are extremely arcane issues. This allows them to drill down and make quite detailed forecasts in response to very specific questions as well as generate broader contextual narrative for clients strategic planning.

With the exception of providing a 'benchmark' against which to gauge other information sources, PRA seems to display all the other contributing factors witnessed to date across the other case-studies:

- It provides context for both public and private sector organisations.
- It can respond to very detailed requirements that necessitate forecasting who, when, where and how.
- It is often quicker, cheaper, and sometimes more fulsome in its product than closed.
- Its product can be used to facilitate communication as well as 'cover' for otherwise sensitive product.
- It can respond quickly to information gaps, changes in tactics of the target, or the emergence of new targets.
- It is most definitely able to produce analysis, or at least a product, which its customers find useful and actionable.

4.2.5 DIS and EUROPOL postscripts

Two postscripts to the DIS and EUROPOL cases are worth mentioning. First, despite promising intentions, DIS was not able to accommodate any further research effort, beyond a preliminary examination of the open source cell, into an examination of the analyst's view of open source exploitation. This was in part due to the extremely high work-load of DIS analysts with Iraq, Afghanistan, and counter-terrorism responsibilities, and in part due to preparation for the reorganisation of their open source effort from mid 2006 onwards. Second, the EUROPOL open source effort, despite achieving trusted indispensability status, was surprisingly disbanded in 2006.

The author's view is that both of these events reflect an organisational cultural ambivalence to open source exploitation; culture trumps efficacy with regard to open source exploitation within these particular parent organisations. DIS, because the institutional environment is somewhat divided between uniformed and non-uniformed cultures, where open source exploitation is not only civilian-run, but, until late 2006, largely outsourced to a commercial corporation. EUROPOL, because the open source effort was for a very long time concentrated in the hands of a successful and effective practitioner.

The lack of engagement with DIS beyond its open source principals, was somewhat alleviated by anonymous discussion with two analysts, who were able to shed some light on the perception of open source exploitation within DIS.[71] Although this is a thoroughly unrepresentative sample size, the reflection of both internal institutional and externally perceived attitude towards open source exploitation was instructive. However, additional contact with the DIS open source cell directors and their open source policy initiatives was maintained through the OSJWG and prior to the DIS open source reorganisation in October 2006, the author was given sight of a classified DIS-wide review of open source exploitation, which formed part of a broader information strategy. In this report, the long and significant contribution of open source exploitation to all-source production was noted, as was the fact that such recognition is not always made so explicit. Similarly, their own interviews with analysts expressed reservations about the institutional attention paid to the treatment of open source exploitation, on the one hand; but broad satisfaction with its effectiveness on the other. For example, notwithstanding the information systems architecture designed to disseminate open source resource to analysts, analysts indicated some disconnection with that system including ignorance of the on-line presence of a well-known commercial content supplier in their field. These accord with the author's own interviews with DIS analysts (see 4.1.1 and 4.1.6). It must be stressed that this review was conducted in 2005/2006 precisely to identify such shortcomings prior to reorganisation in 2006/2007.

Crucially, for this research, the report highlighted six key factors that mark out open source's contribution:

- Context: that is to say historical, geographical, cultural, scientific, technological or other information, within which the nuggets of secret intelligence can be evaluated.
- Cost: it is cheaper than covert collection without entailing the same risks.
- Sharing: it allows analysts to share assessed intelligence more widely.
- Flexibility: it allows collection to move quickly from one subject to another.
- Direction: it enables expensive and fixed closed sources to focus and concentrate where they can be most effective.
- First indication: open sources can often provide the first indication that a subject is worth further intelligence effort.

In both EUROPOL and DIS, but for different reasons, board-level buy-in was not secure: DIS, because they were never convinced in the first place; EUROPOL, because they did not maintain the original and excellent buy-in as board members changed. Arguably, these difficulties are played out in the contemporary intelligence community at large and are as much part of the transition from a Cold War to a 'transnational' era as identifying security threats in the first place. It would seem to the author that, until the decision was taken to return the exploitation of open sources to DIS personnel, their open source effort only really managed level one - cost savings - rather than becoming a trusted and indispensable source of information.

Indeed, the DIS reflects a broader and general misunderstanding of what open sources actually represent. For example, BBC Monitoring input, on the one hand, is praised, but the Internet, as characterised by Wikipedia, is ridiculed.[72] This confusion is culturally reinforced by some senior echelons within the DIS, who display a healthy suspicion of information found on the Internet.[73] This seems to miss three points. First, that the Internet is not the only class of open source information, and certainly not the largest source of information when compared to existing magnetic, film, or analogue data storage.[74]

Second, that all information, regardless of its origin - class, discipline or agency - should be subjected to the same 'principles' of interrogation in order to determine veracity, accuracy, and reliability. Third, it is to seriously misunderstand the Internet as the originator of information, rather than merely the connecting infrastructure between repositories of information Indeed, the principles behind Wikipedia - collaboration and the bringing of many 'eyes' to a problem - have already been absorbed by the US under such efforts as 'Intelipedia' and the Iraqi documents effort.[75] Furthermore, Wikipedia neatly represents the human frailties at play in the pursuit of determining the best representation of reality, and this is largely over things that have happened rather than the more difficult effort of forecasting events yet to happen. It is difficult to assess whether this apparently contradictory approach to the Internet is representative of a more general attitude to open source exploitation. It seems unlikely given that some of the key challenges that DIS is now trying to resolve include: sociological and anthropological understanding; linguistic and cultural understanding; determination of strategic future scenarios; the understanding of contemporary context; contrary 'red team' analysis; international collaboration; 'good enough' versus perfection; and the establishment of warnings and indicators for 'new risks'.[76] The research indicates that these are precisely the challenges best suited to open source exploitation.

The postscript to EUROPOL is equally instructive. While their open source effort achieved a significant degree of success it somehow failed to maintain its indispensable status. In 2006, the EUROPOL 'board' decided that the final location of open source exploitation would be distributed to the analysts themselves. That is to say that the analysts would do their own open source research thus doing away with central open source expertise at all. The open source cell simply failed to continue to educate the board as to the specific tradecraft and broad requirement of open source collection that open source exploitation entails. Not unreasonably, the board saw that analysts had their own desktop Internet access and essentially formally institutionalised open source exploitation with them.[77] Of course, a variety of alternative explanations might be behind the change. It might have been that the contribution and efficacy of open source was so high that

EUROPOL simply directed analysts to exploit it themselves more exhaustively than closed. While this seems somewhat hopeful for advocates of open source exploitation it is not without some credence given that EUROPOL, like NATO, CENTCOM and other international organisations, has a primary function to liaise and share information for a common international good. The 'communicability' of open source (discussed later) is perfectly suited for international collaboration. However, this does not begin to address the issue of where and how closed information is analysed if open has become the predominant form. A 'replacement' policy of open for closed seems as wilfully unscientific as the original unenlightened neglect of open. Alternatively, and more practically, EUROPOL may simply have been cutting costs. However, given that the buy-in explanation is derived from the former head of the open source cell that suffered closure; it seems the more convincing.[78]

4.2.6 UK Intelligence Community Open Source Joint Working Group (OSJWG) including the UK Government Professional Head of Intelligence Analysis (PHIA)/ Open Source Champion[79]

November 2005 was a pivotal point for open source exploitation generally and also a small breakthrough for this research. In the US, Elliott Jardines was plucked from relative obscurity to become the DNI's Assistant Director for Open Source on 8 November 2005.[80] On 16 November 2005, the author presented on open source exploitation to the Royal United Services Institute. Coincidentally, that same day and almost at the same time, the UK's JIC was being formally briefed on the position of contemporary open source exploitation within the Single Intelligence Account and associated intelligence agencies. A few days later, the author was invited to a meeting of the UK intelligence community's Open Source Joint Working Group (OSJWG) to repeat the RUSI presentation. This led to further meetings arranged by the OSJWG to allow the author sight of the OSJWG submission to that same JIC briefing. A third and final meeting, with the OSJWG was held in March 2007 in order to update the author on open source developments prior to

publication of this thesis. Additionally, a separate interview was undertaken with the UK Open Source Champion following the RUSI presentation.

The OSJWG engagement is significant. This committee is made up of representatives from the intelligence community responsible for open source exploitation, including the three SIA Agencies plus DIS. Latterly, JTAC, Cabinet Office Assessments Staff, and SOCA, have also become involved. It has been made responsible under the direction of the Open Source Champion to coordinate UK national open source exploitation policy. Thus, their views collectively represent the intelligence community practitioner view on open source exploitation, in particular the view of the SIA agencies. It is also worth noting that the committee was prepared to engage with an 'outsider' at all; this of itself does seem to indicate a commitment to engage in 'outreach'.

The beginning of support to the UK intelligence community through the formal exploitation of open sources can best be pegged to the creation of the BBC Monitoring Service in 1938.[81] Within the UK intelligence community, the formal exploitation of open sources, notably in support of Sigint, goes back to 1952. The creation of the Open Source Joint Working Group in 2000, representing the three principle agencies of the UK SIA, reflects the present extent to which open source exploitation has become valued and best practised within the UK intelligence community at least. In GCHQ, for example, open source exploitation is undertaken within the purview of Corporate Knowledge and Information Services. The title itself recognises the influences of a broader information-working environment upon intelligence.

Two important factors stand out from discussion with the OSJWG organisation, repeated in EUROPOL but absent in the DIS, which help explain why the development of OSINT within the SIA agencies has been so progressive. First, location, specifically the ethos of GCHQ's new purpose-built circular building (notwithstanding the present accommodation overload)[82] lends an air of all things being directed towards a centre with common purpose regardless of what you do or where you sit in the organisation.[83] This quasi-ideological

approach seems somewhat more significant than the mere physical centrality of an OSINT cell, as in EUROPOL's case. Reinforcing both the physical arrangement and cultural attitude is a structural arrangement, which sees the open source effort centralised in the form of core competencies as well as dissipated out to analysts, where it is most required. Second, the exploitation effort is supported from the 'board' and director downwards. This is in marked contrast to the experience of the VIC/APAN and DIS, whose open source effort is questioned by customers and 'board' alike. In short here, but discussed further in Chapter Five, and like many organisational endeavours, without active support from the top success becomes difficult to achieve or sustain. Equally, the benefits of such endeavours have to be continually demonstrated to the board in order for success to be recognised and support maintained.

The OSJWG demonstrated three contributing factors of open source exploitation that both EUROPOL and DIS also displayed. First - utility - or 'value for money'. If requirements can be met by exploiting open sources rather than the more expensive closed means then it makes obvious financial sense, if nothing else, so to do. Second - context or sense-making - as background briefing to supplement the specific requirement of an analyst's research effort. Third - 'first alert' - open source is the first resource used in response to elucidate or amplify new or breaking news. It is simply the best resource to gear-up quickly at short notice in response to crises.

Indeed, all of the case-studies to varying degree expressed manifestations of these three characteristics of OSINT's specific contribution to the intelligence function. Additionally, discussion with the OSJWG revealed more clearly than other case-studies an additional reason for exploiting open sources of information, which is only really available to organisations that also engages in closed intelligence: open source is also exploited to check the veracity and accuracy of that closed information. The exploitation of open source is conducted by way of a check on information gained clandestinely. It was most clearly emphasised that the finished product of its primary closed function is routinely checked against open sources before being released to its customers if only to avoid

embarrassment, but also to provide value for money. Yet, it was also stressed that open source is also routinely checked against closed in order to demonstrate the inconsistencies and inaccuracies of open source.[84] The Director of the UK's Conflict Studies Research Centre also allude to this latter point, when talking about: "Seeing what is not there, what others would like to hide, e.g. by looking through what they are always pushing to what is not discussed."[85]

Thus, OSINT contributes the benefit of a two-way 'benchmark' against which its primary purpose is measured in simple efficiency terms (inputs to outputs) and its primary product is measured in terms of efficacy (outputs meeting objectives) as a unique information source. Additionally, it demonstrates something more useful than merely the efficiency or effectiveness of the open source exploitation cell on its own. Rather, it attempts to place OSINT holistically within the organisation and aligned with organisational objectives. Thus, it also represents a further tipping point or hurdle in the development of open source exploitation - 'integration.'

Indeed, the integration of open source exploitation into the closed effort is considered so thorough in some agencies, that it has somewhat ambiguously made it difficult for them to distinguish the exploitation of closed and open sources.[86] This statement remains an unresolved and somewhat ambiguous comment, given that open sources are clearly distinguished by definition, activity, personnel and resource establishment in all the other case-studies. Several explanations are possible:

- That they operate a sophisticated knowledge management strategy that really does allow working with all forms of information.
- That they recognise that information, is information whatever the source.
- That they do not distinguish collection methods given their organisational security considerations and classification remit.

Whatever the initial challenges, the capacity for agencies within the OSJWG to become 'superior' processors of open sources of information seems clear. They have some clear advantages: they are part of the Single Intelligence Account and thus central in all respects to the UK IC; their resource in their open source effort is growing, benefiting from the recent increase in SIA resource; as members of the OSJWG they lead development of the UK's national open source endeavour; they have information and communication technological expertise; and they engage in both open and closed exploitation, which affords them mutual comparison.

The case of the OSJWG not only raises discussion as to how best to construct an organisational open source effort, but also how best to conduct a national one. At both levels the discussion necessitates debate about the relative merits of centralising, and thus concentrating open source expertise, versus distributing expertise as close as possible to the point at which analysis is conducted. This question of the locus of open source exploitation is repeated in each case-study. The outcome of such a debate should be some idea as to where an optimum balance between the two resides. This and other related factors such as resource and culture are treated further in Chapter Five. Whether a national open source agency should become an additional responsibility for any one of the OSJWG agencies, for BBC Monitoring, who have similar ICT expertise, or be established independently, has been argued elsewhere.[87] Interestingly, Steele proposed something similar for the US in 2005:

> "In August 2001 General Hayden allowed us the high privilege of briefing the SIGINT Group General and Colonels. **We put forward our view that NSA should become the National Processing Agency, still responsible for SIGINT, but on a foundation of an all-source processing capability able to collect and exploit all OSINT, and fully integrate all operational traffic as well as all HUMINT and IMINT.** General Hayden and Lt Gen Jim Clapper at NGA understand the implications. What has not happened yet is a full and proper hearing on how to actually transform national intelligence by focusing on OSINT and processing instead of secret satellite and human collection. We continue to look through the wrong end of the telescope."[88] (Emphasis added).

At the first meeting with the OSJWG in November 2005, the author presented the high order factors model that represented the state of its development to that point. There was some discussion but little or no challenge, other than emphasising that the 'benchmark check' on closed information by open information can equally be inverted to check open sources with closed. It begs the question whether such benchmarking might usefully be undertaken between Sigint and Humint for example and how such benchmarking is any way different from the all-source process anyway.

Some additional points were made:

- In a typical OSINT cell, the cell director is more likely to be an information specialist than an intelligence specialist and that this had pros and cons to it. Most open source specialists have little intelligence experience *per se*.
- Open source specialists are put 'alongside' analysts as well as retained centrally to form a core competence.
- Effectiveness is measured anecdotally. That is to say they retain evidence of where open source contributes including where analysts are 'pleased' that what they have found through closed means is not also discoverable openly.
- There is a technical distinction made between collection and acquisition. In the intelligence community, collection implies direction, whereas open source is merely acquired or purchased.

At the meeting with the Professional Head of Intelligence Analysis (PHIA) the notion of 'diversity' was introduced as being a significant contributing factor of open source exploitation. In this context, the notion of diversity is taken to mean a diversity of sources of information, sources of expertise, and analysis. If one were to sum the contributing factors, described so far, in one word then diversity would probably cover them all. Because there are so many different open sources of information, context, utility, surge, and analysis can all be more reliably undertaken through open sources than closed. While diversity is undoubtedly a feature of open sources of information, it does not of itself

represent a sufficiently precise contribution to the intelligence function. Rather, it is reflected in all the contributing factors identified so far. In the author's view it would be similar to identifying that the information from open sources was 'open' or 'public'. They are, but that does not precisely explain their specific contribution.

Subsequent to November 2005, the author was given sight of the classified briefing paper on open source exploitation submitted by the Cabinet Office for the JIC's consideration. Additionally, the author was given sight of the OSJWG's classified briefing paper to the Cabinet Office.[89] The papers discussed three key groups of findings. First, the view of the 'functions' of open source exploitation, which might usefully equate to the author's own 'contributions'. Second, the key principles upon which open source should be exploited across the UK intelligence community. Third, the common challenges that open source practitioners face across the intelligence community.

The 'functions' identified by the OSJWG include:

- Context as background for closed intelligence.
- Leverage - to leverage closed through open source techniques such as data-mining or data-aggregating.
- Early warning for closed sources.
- Sense-making of closed.
- Corroboration and validation of closed.
- Target development for closed.
- Unclassified briefing and de-briefing of agents.
- Interviewing of 'uncleared' subject matter experts.
- Sharing of information to liaison officers.
- As rich source simply not available to closed.
- As cross-check to closed.
- For investigation, for example in establishing the identity of individuals.

- Monitoring of low risk countries and emerging threats.

The author does not disagree with any of these thirteen statements. While 'diversity' seems to the author to be too high a 'descriptor' of open source contribution, these 'functions' are beginning to sound like specific examples and thus, an inexhaustible list of what open source exploitation can specifically do rather than how it uniformly and broadly contributes. However, they do reflect the author's own high order factors extremely well, and, if re-organised, neatly fit into the author's own taxonomy when grouped as follows:

- Context:
  - As background for closed intelligence.
  - Sense-making of closed.
  - As rich source simply not available to closed.
- Focus:
  - To leverage closed through open source techniques such as data-mining or data-aggregating.
  - Early warning for closed sources.
  - Target development for closed.
  - For investigation, for example in establishing the identity of individuals.
- Communicability:
  - Unclassified briefing and de-briefing of agents.
  - Interviewing of 'uncleared' subject matter experts.
  - Sharing of information to liaison officers.
- Benchmark:
  - Corroboration and validation of closed.
  - As cross-check to closed.
- Utility:
  - Monitoring of low risk countries and emerging threats.

Of particular use is the notion of 'crosscheck', which more accurately reflects the process of comparing closed with open sources (and vice-versa), than the author's term 'benchmark'.

Three of the statements seem to stand out as having no discrete factor in the author's model so far constructed: 'Target development for closed'; 'monitoring of low risk countries and emerging threats'; and 'early warning for closed sources' might usefully be represented by the notion of 'surge'. When the unexpected happens, and therefore by definition no useful body of intelligence exists upon which to make decisions, it will be to open sources that decision-makers will turn in the first instance. For example, it would be reasonable to suggest that hostage negotiators deploying to remote parts of the world not routinely covered by a closed intelligence capability would welcome any information (and quickly) to help them: maps, key personalities, meteorology, communications detail, communications infrastructure, culture, linguistics, to name a scant few can all be supplied by open source means more easily than closed assets. Arguably, open source has been the only means to support such rapid action.[90]

The 'principles' identified, include:

- 'Acquire not collect' - because the sheer volume of information coupled with the resource available to work it, indicates that a different attitude to information working might include collecting just in time rather than just in case.
- 'Alongside the customer' - this is because customers want a tailored product rather than a generic, uniform, centralised one, and because open source exploitation differs in its acquisition, delivery and presentation. Consider the law enforcement need versus the intelligence need.
- 'Do it once for the community' - because it makes commercial sense if not maximising resource efficiency.
- 'Rotate specialists' - as part of a professionalisation project for open source specialists as well as an education process for the rest of the intelligence community.

- ‘Joint approach’ - again as part of a professional project, resource efficiency, and community education approach.

The ‘challenges’ identified, include:

- There is no one organisation within the UK IC that is setting priorities for OS acquisition.
- There is a distinct lack of shared infrastructure for the delivery of open source to the JIC community.
- There are business constraints, notably financial, particularly where buying commercial product is concerned.
- "Many commercial open source systems do not provide a secure means of searching because they are accessed externally outside our firewalls. In some cases it can be brought inside but this is technically unsafe and therefore not possible to be made available to desktop."
- "The opportunity to influence the commercial market is limited - we are only one customer among many."
- "Commercial organisations do not consider the needs of security. For example, they put everything on line, when intelligence organisations would prefer material on CD-ROM as it is considered more secure for their purposes."
- Remember that in the open source world only BBCM is tasked by their respective sponsors, otherwise the IC do not task for open source exploitation - thus OSJWG is not a tasking authority - they are an acquiring and exploiting 'authority'. Requirements and priorities remain crucial though.

Finally, specific recommendations were made for the UK intelligence community to adopt with regard to open source exploitation:

- The OSJWG should increase and build upon its procurement and acquisition effort of open sources, because influencing the open source market is difficult and limited other than through cleared contacts within these organisations.
- There should be a short-term secondment of OSINT info specs into the Cabinet Office Assessments Staff in order to train researchers and assessments staff in OSINT exploitation.
- Increase the build up of the IT infrastructure in conjunction with others in order to export open source product around the intelligence community.
- Include the FCO Research and Analysis Division, Cabinet Office Assessments Staff, and JTAC in the OSJWG. (To the author's knowledge the latter two have now been included).

These principles, challenges and barriers to achieving them are discussed further in Chapter Five (5.1). The OSJWG's own recommendations should be considered alongside the author's recommendations in Chapter Six (6.8).

At the final meeting in March 2007, the OSJWG identified some key changes to open source exploitation that had been effected since submission of the 2005 positioning paper to the JIC:

- The Open Source Champion has issued guidance notes for analysts on open source exploitation for all analysts.
- Interestingly, with regard to tasking, the Open Source Champion is examining the proposal of issuing certain tasking requirements simultaneously 'down' open and closed channels.
- Broad training on the principles and significance of open source exploitation has been increased for analysts.
- Specific training on utilising the Internet has increased. Some 1,000 personnel from across the entire intelligence community have gone through the 'search smart' programme.[91]

- There has been greater involvement of OSJWG members in 'higher' requirements and process working groups and sub-working groups. Open source representation in the internal processes of the intelligence community is spreading.
- For most agencies on the OSJWG this has also meant both some increased budget and personnel resource. It is unclear whether this is the case for DIS, although from October 2006 to January 2007, they went through a complete change of ethos regarding open source exploitation.

Interestingly, the DIS representative summed up the contemporary situation for open source as at 2007: "We no longer have to hold our ground."[92] There is a greater awareness, a greater recognition, and a greater understanding for open source exploitation across the intelligence community. They are making their case.

Two further points were emphasised: first, that the OSJWG belief is that open source expertise should be dispersed but networked around the community rather than separated and singled out in stand-alone cells; second, and similarly, that an open source 'agency' similar to the US Open Source Centre was counter-cultural to this embedded notion.

4.2.7 Summary of PIBs and OSJWG

Hazard Management Solutions and Exclusive Analysis, like many other private information brokerages, can do what they do as a result of two important developments in the early 1990s: the transformation in ICT and the reduction in the size of Cold War Armed Forces. The latter created the migration of experienced personnel, including intelligence, from the public security sector to a nascent private security sector that has grown inexorably to their present day substantial engagement with DOD and NATO in Iraq and Afghanistan. The former gave this new sector information upon which to forecast, plan and operate. Interestingly, while PRA also exploits the ICT transformation, it relies heavily on other traditional media formats, while exploiting a remarkably narrow capability gap within the public sector law enforcement community.

Additionally, and where they all combine, is in their translation, interpretation, and assessment of the information available to them into a final product, which is perceived useful to decision makers elsewhere. This product is useful for a variety of reasons that the research has already seen amongst the preliminary investigations: it is communicable because it is openly derived; it fills a gap in information not found elsewhere, both contextually and in precise detail; it provides information quickly and, significantly, more quickly than a customer could do itself; it is simply cheaper to 'buy' it in from outside their own organisation; the interpretive expertise - technical, cultural, and linguistic - is not available within their own organisation; the analysis contributes to an organisation's own or other analysis. They do what they do because they can. What they do is purchased because it fills a perceived gap and is thus considered valuable.

If the emergence of the Internet combined with the end of the Cold War gave them the opportunity, then 9/11, the resultant Global war on Terror (GWOT), and the 2003 war in Iraq, proved to be the catalyst and environment for a 'parallel' private sector engagement in most matters concerned with security.[93] Open sources of information are virtually their only information sources. However, the combination of sufficient information with analytical expertise, when added to the other benefits of open source exploitation already discussed in Part One above, proved invaluable to the traditional public sector customers of intelligence collection. Arguably, and perhaps contrary to Steele, it was the contraction of the public security sector, rather than any intrinsic value, that finally gave life to this new scion of intelligence - OSINT - in the private sector. This raises a significant question discussed further in Chapter Five - where is OSINT best practised?

All of these PIBs broadly reflect the shifting responsibility for the conduct of security; specifically the increasing conduct of traditional intelligence functions by the private sector. Their activity, and an increasing number like them, does not represent a wholesale migration of intelligence away from the public sector and into the private; but it does represent a significant transformation in who does it and for whom. This transformation includes a widening intelligence community of collectors and analysts, together with a

widening customer set who feel that they benefit from the service. It also represents a shift in how it is done in the sense of why, as well as context in the sense of secrecy and bureaucracy. The commercial sector has felt increasingly poorly served by government agencies, while at the same time perceive that they are more, or as likely, to be targets of risk and uncertainty as the public sector. Equally, public sector agencies utilise both the private sector capability and capacity in the absence of its own.

The preliminary research identified eight high order factors: utility; analysis; context; 'first alert'; benchmark; focus; surge; and communicability. These factors were nearly all repeated in the examination of case-studies selected to develop the model. The notion of 'first alert', advocated by both DIS and the OSJWG, was dropped at this stage because for some of these case studies the term is meaningless given that open source is their only alert mechanism. Moreover, first alerting is not necessarily the exclusive preserve of open sources. More appropriately, this term can be incorporated into the notion of surge, whereby information, when required quickly, against a requirement, in a crisis, and in the absence of closed information, is sourced in the first instance by recourse to open sources; the first port of call. Finally, the high order factor - benchmark - is considered insufficient to describe the notion of checking closed against open, while neglecting the potential that the OSJWG point out of also checking open against closed. The ability to cross-check one against the other is a useful additional concept.

Again, not all the case-studies reflected the factors evenly, and the research was not set up to determine such a pecking order. However, the seven high order factors to take forward to the model confirmation stage might usefully be stated here as: context; utility; cross-check; focus; surge; communicability; and analysis.

4.3 Part Three: Confirming the model – US Army Asian Studies Detachment (ASD)

The ASD case-study was initially intended to be the final development phase of the research's high order factors model. However, following the tacit approval given to the model by the OSJWG, it became clear that the data obtained from the ASD case-study might usefully be viewed as the first test of the model's generalisability. This case-study allowed the author unlimited access to all personnel, systems and processes for a five-day continuous period in January 2007. The data obtained from the ASD comprehensively supported the model's description of open source exploitation.

The ASD has become the DOD's exemplar for open source exploitation, yet, nowhere does the DOD say why in the sense of describing how it contributes.[94] Indeed, the ASD was cited as the 'model' open source organisation for the Army in the December 2006 Field Manual Interim 2-22.9: Open Source Intelligence, which is now the US Army's doctrinal 'gospel' on open source exploitation.[95] The ASD is situated under command of the 441st Military Intelligence (MI) Battalion, part of the 500th MI Brigade, which is seconded to the US Army Pacific (USARPAC) and ultimately US Pacific Command (USPACOM). However, and perplexingly to ASD, it is controlled by the DOD's Intelligence and Security Command (INSCOM) for administrative and budgetary purposes. Additionally, the DOD's Defense Intelligence Agency (DIA), which is broadly responsible for DOD strategic intelligence where INSCOM is responsible for Army strategic and operational intelligence, has established a 2-star Senior Contracted Staff post - Chief, Defense Intelligence Open Source Program Office (Mr James G Noone) - specifically to direct and consolidate open source exploitation within the DOD. Furthermore, over the previous twelve months (2006) the ASD received close interest community-wide following the November 2005 creation of the Open Source Center (OSC), the creation of the post of Assistant Director DNI for Open Source (ADDNI/OS), and the issue of the July 2006 Intelligence Community Directive 301, which lays the DNI's foundation for a federal approach to open source exploitation - the National Open Source Enterprise - under the auspices of the ADDNI/OS (Mr Elliot Jardines).[96] The OSC were regular visitors to ASD

during the course of 2006. As the federal focus for open source exploitation, the OSC represent professional colleagues if not professional direction for open source exploitation policy, doctrine, training, and standards.

The ASD was originally established in 1947 as the 'Research and Analysis Group, Town Plan Group, and Cartographic Unit' of the G2 Geographic Section under General MacArthur's General Headquarters in Tokyo. The unit was re-located to Camp Zama in 1974 and became known as the US Army Asian Studies Detachment from October 1981. The Asian Studies Detachment is in many ways a quirk of history. Like the liaison missions of Cold War Europe, it is a remnant of the Second World War. What was to all intents and purposes a liaison unit at its outset soon came to recognise and reflect the unique position afforded to it for the conduct of intelligence operations. The hiring of repatriated Imperial Army officers hints at the intelligence role. Yet, as its Director acknowledged, it is unlikely that the ASD as presently constructed would be established today. Given the increasing interest and evaluated returns on their product, one might be rightly tempted to ask - why not?

The key issue for ASD is political in that it is clear to all parties that ASD is a national asset, producing 'world-class' product, paid for by the Japanese government; yet under command of a battalion commander. This is reflected in the command and control structure: operationally they are directed by the PACOM via the 500th MI Brigade and 441st MI Battalion; administratively and financially they are controlled by INSCOM; strategically they are gaining interest and recognition from the DIA; and professionally they are increasingly likely to come under the purview of the OSC. It is challenging, to say the least, to serve so many masters. Yet, it is also reflective of the fragmented understanding and utilisation of open source exploitation as well as a growing (re-growing to be precise) contemporary interest in open source collaboration at the national and federal level, which seems to be running ahead of ground truth.

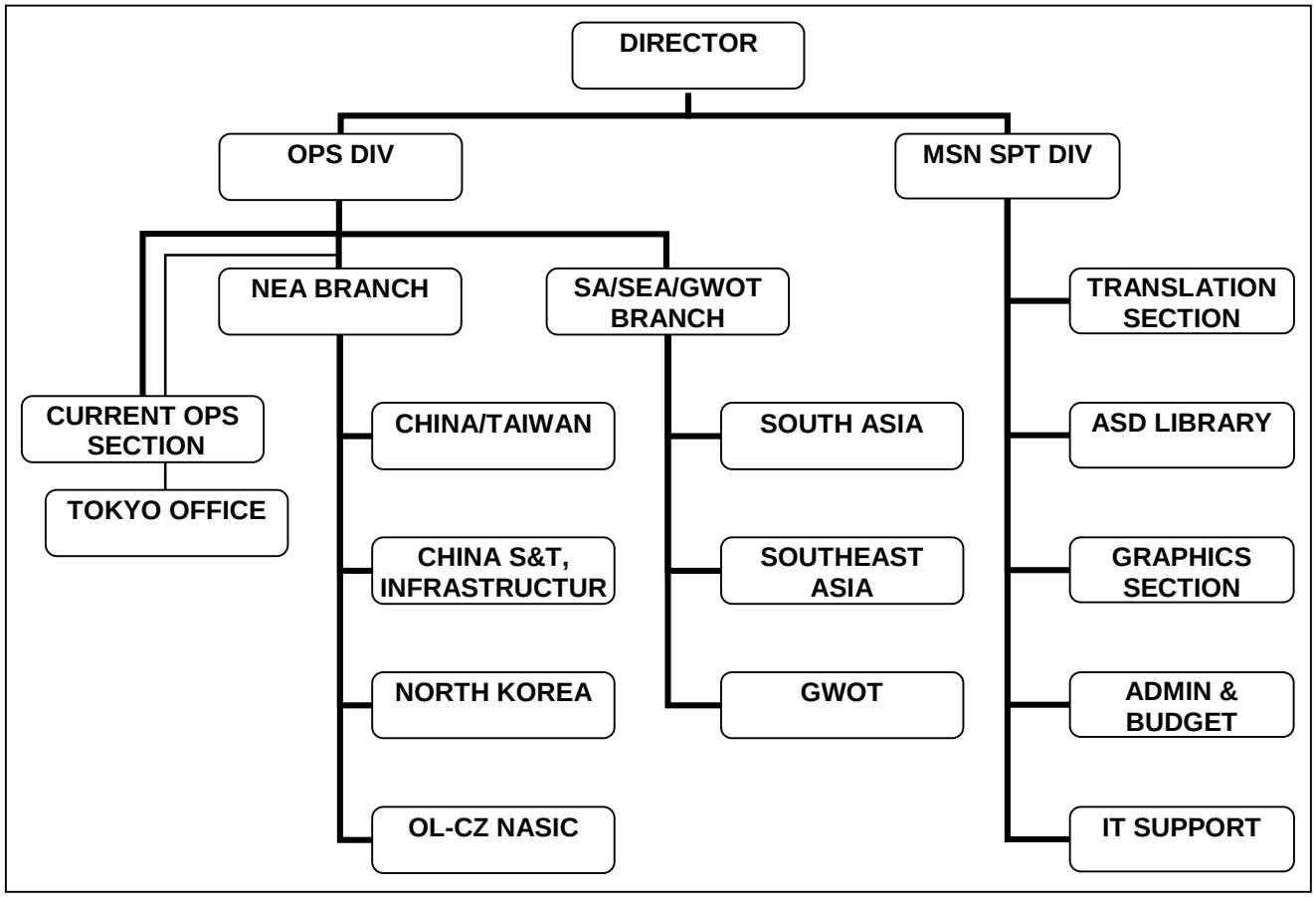
4.3.1 Organisation and personnel

The ASD is a US Army asset. It serves as the model of open source exploitation for US Army Combatant Commands (COCOMs) and Army Service Component Commands (ASCCs). Much of the process and principle in evidence there, is replicated at the US European Command (EUCOM) Joint Analysis Centre at RAF Molesworth, UK.[97] Although it is a strategic and theatre-level asset equivalent to the open source cell at US SOCOM or the 'Naval Open Source Intelligence' effort, which was not researched, it is by far the most significantly resourced open source effort with the US military.

The ASD is established at approximately 96 personnel strong. 75 of these personnel are locally employed Japanese civilians paid for by the Japanese Government. Approximately 15 (of the 90) personnel are Department of the Army Civilians (DACs), who effectively coordinate, lead, and quality control the ASD's final product. Many of these DACs bring with them private sector and public sector experience from various countries. The DACs are all Japanese linguists. The remainder (six) belong to other organizations co-located with or augmenting the ASD: one or two US civilian private contractors work on IT content, technical editing matters, and reports, in order to support ASD's digital presence; and three or four represent other intelligence agencies at the ASD including US Air Force and Navy using locally employed civilians. See figure 4.2 below.

All together, the ASD has language expertise in some 15 plus pertinent regional languages: Bengali, Burmese, Chinese, Indonesian, Japanese, Khmer, Korean, Hindi, Malaysian, Nepali, Russian, Tagalog, Thai, Uygur, and Vietnamese, as well as Russian.

Figure 4.2 Asian Studies Detachment organisation chart



Source: Asian Studies Detachment, 2007.

Until the mid-1980s, the US government funded all salaries, including those of the Japanese workers on base. In the mid 1980s the US asked Japan to pick up a greater portion of its defense cost through payment of the Japanese workforce salaries. Indeed, the Japanese government now pays the salaries of all Japanese workers on US bases across Japan under the US Forces Japan Master Labor Contract. As the unit's analysts, translators, librarians, and administrative support personnel, the Japanese personnel undertake most of the ASD's collection, analysis, and reporting effort. Within this number there is a small section of locally employed civilians responsible for the acquisition of 'hard to obtain' material from target countries such as North Korea.

4.3.2 Mission

The ASD describes its mission as: to collect, analyse, and report publicly available information from foreign open sources in response to theatre and National level intelligence requirements.

The unit exists primarily to support the intelligence needs of USARPAC and PACOM, although its product serves all Military Services, COCOMs, DOD intelligence agencies including the DIA, the National Ground Intelligence Center (NGIC), and the US Air Force's National Air and Space Intelligence Center (NASIC); non-DOD customers such as the DNI OSC, the FBI, the Department of State; and nongovernmental strategic think tanks. Topics range from North Korean underground facilities to Chinese Peoples Liberation Army Air Force air and space science and technology developments, to country infrastructure and avian flu monitoring.[98] In short, directly or indirectly, the ASD supports most members of the US Intelligence Community across a vast array of topics. As such, it represents an optimum case-study of US open source exploitation. Indeed, the ASD sets as its own objective: to strive to set the standard for providing timely and value added reporting on Asia, derived from the fullest possible exploitation of foreign open sources.

4.3.3 Activity and product

> "You cannot task Sigint to get Humint; but you can task OSINT to do all the others (Ints) to a degree."
>
> ASD Interviewee 3

The ASD should not be viewed merely as a translation unit, or a media exploitation unit, or a collection cell. To a degree, it is a discrete intelligence unit in its own right in the sense that its analysts 'collect' materials, 'process' relevant information relating to the intelligence requirements, and create products in answer to these given requirements.[99]

The ASD subscribes to approximately 300 international publications in hardcopy and digital format. Where open source material cannot be acquired by subscription then these

materials are acquired through ‘memberships in international research and friendship organizations’ as well as by direct purchase from foreign bookstores and publishing houses.

Their principle product is the ‘Intelligence Information Report’ (IIR). These intelligence information reports are, to all intents and purposes, intelligence assessment product. The reports are written in Japanese by the analysts and only then translated into English by the ASD Translation Section. These are then checked for translation, final editing, and formatting by the DAC Reports Officers within the two respective ASD Branches. They are then published as intelligence product.

With the exception of some Defense Attaché reporting, some regional embassy-based media exploitation cells, and regional OSC (formerly FBIS) units, the ASD is the only unit in the US Army that synthesizes and cites a large number of open source references in an intelligence report format similar to research papers or essays. (The Foreign Military Studies Office (FMSO) does a similar thing but to a completely different set of requirements for the Deputy Chief of Staff Intelligence at the US Training and Doctrine Center, Fort Leavenworth, Kansas).

In addition to the IIRs, the Current Operations Section produces three current intelligence reports: a daily ‘Force Protection and Situational Awareness Report’; a daily ‘Areas Surrounding Japan OSINT Report’; and a ‘PACOM News Clips report’. These are all essentially e-mail products compiled from news excerpts extracted from foreign media websites throughout the PACOM’s Area of Operations. While the IIR is strategic in nature, the current intelligence reports are more tactical, providing US forces stationed or deployed in the region (and ‘other travelers’) with current security-related open source information. All of these products are available on the ASD's classified and unclassified websites. Additionally, the Force Protection and Situational Awareness Reports are posted on the DNI OSC’s website, the FBI-Honolulu's Law Enforcement Online website, the FMSO’s World Basic Intelligence Library (WBIL), and Army Knowledge Online’s (AKO) Intelligence Knowledge Collaboration Center.

Unsurprisingly, North Korea, China, and terrorism are high priority targets for the ASD, reflected in the two branches main efforts. They do not target South Korea as there are US forces based there who can examine South Korean affairs. However, US forces cannot examine North Korea from South Korea because South Korea does not allow any imports from the North. Thus most North Korean material has to be acquired in other ways. Here the ASD's Tokyo Detachment Office comes to the fore. On the Internet, where direct monitoring of North Korea is difficult, they go indirectly via Taiwanese and Chinese sites that themselves 'comment' upon North Korea. Connected to the North Korean scientific and technical periodicals, in terms of degree of usefulness, are the Chinese People's Liberation Army's military regional newspapers (e.g. Renmin Jundui and Zhan You Bao), which are available by subscription. They come in hard copy, partly because these tend to be fuller versions of similar content found over the Internet, and partly because this can be the only way they are made available.[100]

4.3.4 Intelligence Information Reports (IIRs) and evaluation of effectiveness

> "It's only valuable if the user finds it valuable."
>
> ASD Interviewee 2

IIRs are the primary product emanating from the ASD. At the top of each IIR is the DIA-imposed comment: "This is an information report not finally evaluated intelligence". This is deliberately designed to press the point that OSINT analysis is not all-source intelligence product, but an initial interpretation of raw information rather than finished, vetted intelligence. The ASD interprets information literally and metaphorically in the intelligence sense. Thus IIR as a term is extremely meaningful of itself. It essentially means interpreted information put into the intelligence process.

The DIA originate DOD 'Humint collection requirements' (HCRs) via the Secure Internet Protocol Router Network (SIPRNET). The DIA then stipulates that, for the entire DOD, 15 percent of responses to HCRs (all reports, including but not only IIRs, generated as a result of an HCR) are to be evaluated by the originating analyst (generator of the original

HCR) from the originating agency. It is a goal rather than a mandate. For example, a former Commander at NASIC directed that all IIRs would be evaluated, whereas a more recent Commander stipulated that no IIRs would be evaluated. Returns on reports generated against HCRs are collectively termed - 'evaluations'. All such evaluations on IIRs follow a set format constructed using 'prosigns' in a format established by the DIA.[101]

Interestingly, although the DIA goal is to generate 15 percent evaluation by HCR taskers, the ASD has, on average, generated a 36 percent return annually since 1997 and 63 percent in 2006. This raises a whole series of possible explanations: maybe ASD work is easier to evaluate; maybe the OSINT reports are so useful that an 'obligation' to respond is established; maybe there are favours being curried between analysts and ASD OSINT (for example the NASIC section get regular, high evaluation returns because they are effectively created by their own personnel within the ASD); maybe 2006 reflects the increasing OSINT interest since the establishment of the OSC in November 2005. Furthermore, because of the somewhat bureaucratic nature of the evaluation format (to fit consigned 'prosign' fields) they are not user-friendly, highly proscriptive and time-consuming. Finally, if originators of HCRs know that they have to report on 15 percent of the returns to their own HCRs, they may be selective in their creation at the outset, possibly even knowing that OSINT will have an answer, which they can use and further disseminate.

Thus, the evaluation system is highly nuanced and, however objective its intention, is quickly susceptible to the sophisticated interpretations and manipulation by barely detectable human factors. The possible permutations of this aspect of the process are legion but worthy of further investigation given the importance attached to, and will be increasingly attached to, the use of metrics.[102] It has not been possible to determine the precise reason for such a high evaluation return, or whether other agencies and disciplines receive similarly favourable treatment. Suffice to say, for this research, that it happens.

To complicate matters further, it is only the Humint production cycle (not the other Ints) that is evaluated in this way. There is no equivalent for OSINT. The ASD use this system

because they can monitor and respond to the HCRs posted to the SIPRNET, whether they are specifically tasked or not. Interestingly, this procedure begins to represent the initiative suggested by the UK's HPIA above (4.2.6), whereby intelligence requirements are passed out to all intelligence disciplines rather than directed to particular agencies.

The important point is that these evaluations represent the principle method by which ASD 'measures' itself. This measurement is effectively longitudinal i.e. against itself over time rather than against or in comparison to any other agency or intelligence source. In this regard, the measurement of effectiveness is genuinely useful to the improvement of product within the ASD for the benefit of ASD's customers. However, the effectiveness remains internal to the intelligence community - intrinsic and customer focused rather than extrinsic and purposeful in any policy-oriented way. The sole exception is a 'Grade A', which is defined as 'of major significance' and understood by the ASD (ASD Interviewee 1) to signify a policy change or a change in the way of thinking about the subject matter.[103] There is no 'set' evaluation report format that recognises the specifically intrinsic contribution of OSINT. Arguably, the writer of the evaluation should not be 'pigeon-holed' into yet more bureaucratic formats, and anyway, beyond the ASD, the evaluation returns are often uninformative either up or down the chain.

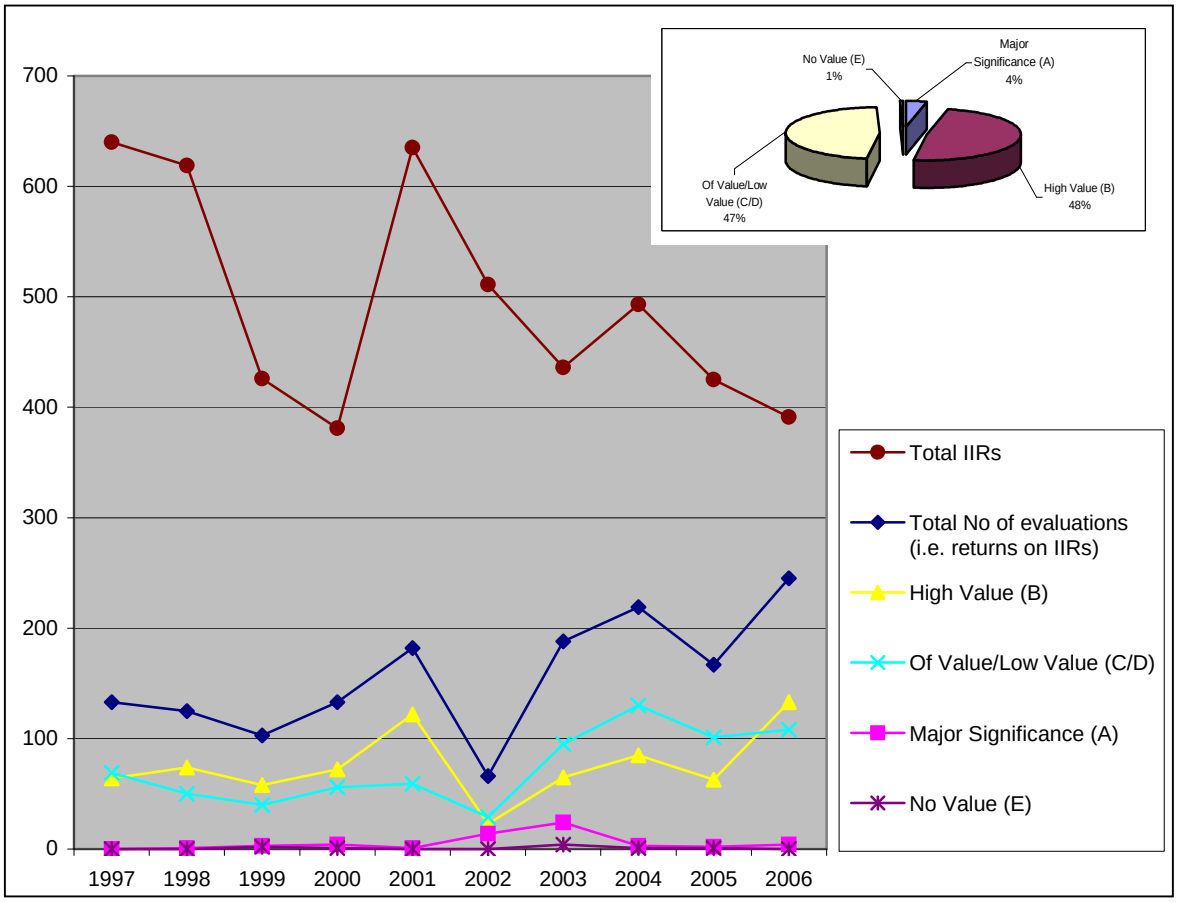
4.3.5 Quantitative data

Unlike any of the other case-studies, the author was given access to two data sets that could be interpreted quantitatively: first, the overall 'evaluation return statistics' from customers; second, the text of the entire 1,183 sanitised/unclassified 'evaluation return reports' that are given to the analysts and from which the evaluation return statistics have been calculated.

The evaluation return statistics for the fiscal years 1997-2006 inclusive are instructive although difficult to discern any clear trends. Broadly the number of IIRs submitted has declined, while the number of 'evaluations' on the IIRs has increased. The proportion of those evaluations returning a grade of 'major significance' or 'high value' has also risen,

but imperceptibly. The years 2002-03 are somewhat inconclusive. On balance one might begin to suggest that the overall picture is one of increasing quality of output. See Figure 4.3 below and Appendix B.

Figure 4.3: ASD total evaluation returns 1997-2006 (inclusive)



Source: Asian Studies Detachment, 2007.

However, given that generation of evaluation returns on IIRs is ultimately an analyst's prerogative, an evaluation return is not necessarily the true or definitive indicator of IIR effectiveness; but it is an indicator.

4.3.6 Challenges, issues and future prospects

The emergence of the Internet has transformed the ASD's OSINT techniques and procedures. Approximately 70 per cent of the ASD's cited sources currently consist of Internet-derived information. This proportion has been steadily increasing. It is likely to increase further as the ASD is keen to meet the challenge of increasing Internet coverage. At the same time the ASD has to protect its Internet research from external and internal threats to its operation. To this end, in 2006, the ASD completed installing and standardizing the use of the Intelink-U system on all of its computers for Internet searches. This system supports increased operational security measures while not compromising its ability to conduct overt collection. Additionally, the ASD has researched the possible exploitation of audiovisual media utilizing tools, which enable continuous real-time monitoring, transcription, and machine translation of foreign-language television broadcasts, but have decided that it was not presently feasible.

A key issue to understand is that the ASD is an intelligence organisation in its own right in that it collects, assesses, and disseminates product in its own right. Obviously it responds to requirements in the first instance from consumers and customers of its product. However, this part of the process - tasking - is frustrating for ASD. Their 'line-managers' do not clearly understand the ASD capability and often mis-task; whereas the more senior tasking agencies understand the capability, but do not have effective control.

Both the Director and Deputy Director saw no advantage in outsourcing the unit, although they recognise that it could be done; indeed that it could be commercially oriented. There are downsides: first, a strong link with the customer - US Government - that allows for the nuances and specific tasking efforts of the military. Second, in the specific instance of the ASD, it is virtually paid for by the Japanese Government.

4.3.7 Open source contribution

Collectively across the organisation and entire interview set the following extracted comments were identified as typically representing open source contribution as ASD understand it. Alongside, in square brackets, are the high order factors as already understood in the model developed from other case-studies:

- "It paints a fuller picture. Open sources generates context. It summarises a subject for the analyst." ['Context']
- "Unclassified information is of value in its own right because of its wider use. It allows dissemination to a wider audience." ['Communicability']
- "It is less costly and more economical than other Ints. It saves time for analysts. There is simply more information available in open as opposed to closed sources." ['Utility']
- "It checks or confirms what we have seen in other Ints. It confirms what is known secretly. It adds value or corroborates other sources. It can be compared and contrasted with closed." ['Cross-check' (and 'Utility')]. It is worth noting that this comparison argument is universal and in the main it is expressed as a check on closed rather than the other way around.
- "It allows them to work on mid or long term analysis although presently 'current-int' is in vogue." "It allows independent analysis. Open source lends an all-source capability as well creating opportunity for indicating what should be important." This is not just collection and analysis but also policy. ['Analysis' (and 'Context')].
- "It prompts further questions from the analysts. It alerts the analysts to issues and subjects they had not considered or previously 'asked' for. It also deals with the nuts and bolts." ['Focus']
- "It fills gaps in requirements e.g. specific technical requirements." ['Surge'] "The 'scoop' syndrome i.e. 'information seen for the first time' comment in evaluation returns. Every now and again it produces a scoop - the 'sexy' stuff." Scoops are of course not peculiar to OSINT.

The following three quotes from a visiting customer/analyst to the ASD are instructive:

- "I don't worry about it; it will come up in open source sometime soon."
- "ASD has better sources than the intel people!"
- "ASD does something that no one else is doing"

4.3.8 Summary of ASD

"Watch this space"[104]. ASD will more than likely move to be a DIA if not OSC asset, reflecting its more 'national' capability. This does not sit comfortably with the fact that it would not be established if it did not exist today. The paradox reflects the lack of political will to engage with open source at the 'grown-up' level and part of that is because open source struggles to demonstrate efficacy in comparison to the other 'ints'. Once again, the cultural proclivity to 'closed' holds sway. When combined with structural mis-management then open source is relegated to second-cousin status.

The ASD is simply not a collection agency, a news exploitation centre, or a translation unit. It is all of these and more. It is essentially a national IC asset with customers across the spectrum of Federal security, defence and law-enforcement organisations, generating intelligence product of global pertinence, largely paid for by the Japanese Government, under immediate command of a Battalion Commander. It is a curiously paradoxical position. However, the ASD has a particular political anomaly in that it is closely pegged with US-Japanese relationships.

Notwithstanding the US-Japanese arrangement, the ASD seems mis-sited and misused by its own executive agency. This is largely due to a misunderstanding at senior levels within its own executive as to the efficacy of an open source capability; possibly even a fundamental understanding of open source intelligence in the round.

The following ‘recommendations’ were left uncommented upon in their corrected returns of my notes:

- An examination of the entire intelligence tasking and requirements practice needs to be undertaken at DIA level for the DOD as a whole; to include OSINT.
- Failing this, a tasking and requirements system pertinent to the growing utilisation of OSINT needs to be established DOD-wide.
- Secondary to this issue is striking the right balance between centralisation of OSINT exploitation in order to concentrate resource, avoid duplication and enhance working practice, versus the decentralisation and dispersal of resource in order to meet specific customer requirements.
- The ASD should be positioned more appropriately to its role. Whether this is as part of the national open source enterprise or part of a DIA/DOD effort remains to be seen with the recent arrival in post of Mr Noone as DIA open source ‘advocate’. As presently constructed and manned it is probably best placed to continue to serve the military requirement. Yet, as presently positioned it is stymied by an unimaginative and bureaucratic chain of command management. The US-Japanese sensitivities suggest that geographically and politically it should remain in Japan for the foreseeable future in support of beneficial US-Japanese relationships (which of course it may be a significant contributor to). However, from the US IC perspective it seems ‘embarrassingly’ (for the US) under-funded and under-resourced. Given the growing importance of the region exemplified by North Korea and China, it seems an opportune moment to boost the geo-political and military understanding of a complex (rather than merely complicated) environment.
- The ASD could do so much more were it appropriately resourced and funded. There is clearly opportunity with the additional staff to generate product of geo-political significance not unlike the DOD Centers for Regional Security Studies. Such a geo-political role may of course conflict with OSC work. Alternatively, it may provide a competing hypothesis for all-source assessment.

- The ASD is an analysis effort rather than a collection effort and should be treated or recognised as such. This is of course not to say that it is final all-source intelligence assessment product.
- The evaluation reports should be centrally compared and contrasted with other intelligence reports so that something more meaningful, relatively, can be deduced from them.

4.4 Part Four: Other common features of OSINT exploitation

Some common structural and cultural themes emerged during the data collection phase and recur throughout the thesis. Whilst they do not necessarily represent the main thrust of the thesis question they do shed considerable light upon the context in which open source has emerged and is being exploited this time around. They also represent some of the key issues that national open source endeavours are wrestling with. Thus, they are raised and aired here at least and discussed further in Chapter Five, and Chapter Six, where recommendations are offered.

4.4.1 OSINT's 'place' in the intelligence process

It seems important to establish exactly where the intelligence community exploits open sources. Certainly, open source information is exploited by all the intelligence agencies that this research engaged with.[105] Some exploitation is undertaken internally by discrete in-house open source 'cells', some is 'bought-in' as 'finished product' from external commercial or other providers, some is done by analysts themselves, and some is done through a combination of all of these. The dilemma that all the public sector case-studies demonstrate is where best to place their own open source exploitation assets. Should they be centralised for maximum effect, distributed to the point of production where requirements are answered, or some combination of the two that is inevitably more demanding upon resource. All the public sector case-studies also demonstrated some

frustration with the confines of a closed environment. This remains the case as was emphatically confirmed in February 2007 by analysts that the author presented to on the Cabinet Office Analysts Course. Thus, it is not just where open source resource is placed within a closed agency, but, also, whether open source exploitation be conducted effectively within the constraints of a secure environment at all? Speed and utility certainly seem to be traded for security, while a compartmentalised and classified culture actually detracts from an all-source production and dissemination capability.

It is also instructive to observe how open source is collected. Interestingly, both GCHQ and HMRC affirm that it has become difficult to 'separate out' data collected from open means and data collected from traditionally clandestine means.[106] On the face of it this seems strange since they both have dedicated open source exploitation efforts. Yet, this conundrum reflects several dimensions of the difficulty in distinguishing exactly what is and what is not open source exploitation. For example, just because data has been collected from an open source does not mean that it remains unclassified in a closed agency. Equally, the collection of open source material is often done anonymously and thus clandestinely. The US Intelink-U system is being fitted with an 'anonymising' capability, while commercial open source efforts use software to conceal the path of their digital enquiry from PC through Internet Service Provider to the target web data server. Rationalising secrecy and security in open source exploitation still remains problematic.

Somewhat more intractable is an attempt to determine who does what with the open source material that is collected. Should cultural, linguistic and technical expertise, that is necessary to conduct discerning collection in the first place (notwithstanding requirements set by customers), be corralled in some way at the collection stage, or be utilised to conduct analysis as well? Again, there might be a useful halfway house position that, like other intelligence disciplines, sees their product interpreted at least before going forward to final all-source assessment.

On the one hand both EUROPOL and DIS had very clearly defined and separate open

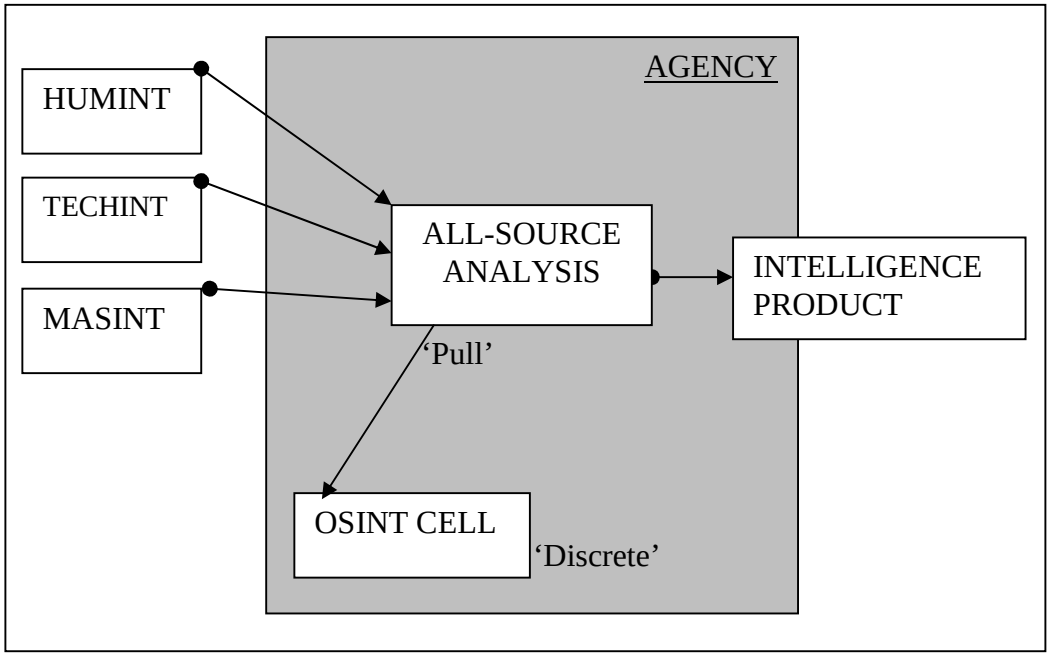
source exploitation cells. Similarly, ICTY, apart from military led operations in-country, almost exclusively utilise open source exploitation, partly because the data they exploit is historical media output, and partly because the use it is put to is evidential and thus, by necessity has to be 'useable' or communicable in court as evidence. On the other hand, the OSJWG's aspiration is to distribute open source expertise to project teams, physically sitting them alongside analysts so that questions and requirements can be addressed 'there and then'. Similarly, while the SOCOM open source effort is physically concentrated and centralised in one place, its personnel are constantly out and about with their customers. Coupled with an obvious 'can-do' attitude, an impression of open source ubiquity is created within SOCOM's wider intelligence effort. Then there are stand-alone open source efforts such as BBC Monitoring and the ASD, where history and resource allow them to function in a semi-independent manner, supported by the wider intelligence and security community in financial and resource terms, but independent in terms of how they conduct their work. Finally, the private sector open source efforts are entirely independent, but of course outside the intelligence community; at least formally so.

Thus, two variations in the 'placing' of OSINT exploitation have emerged: first, as discrete or 'bolt-on' cell, which occurs in an all-source environment; second, as embedded, distributed, threaded or 'enmeshed' activity, which occurs in a single source agency. Of course, the nature of the intelligence organisation - single or all-source - is immaterial. The choice to either centralise or enmesh an open source effort is a deliberate one based upon resource constraints, demonstration of efficacy to the board by the open source effort at the outset, and a degree of enlightenment at board level to the way that the information business is moving in a wider world. That a single source agency might go that way seems largely reflective of the sophistication of the agency and its internal debate between appropriate structure and receptive culture to a changing information environment, rather than any self-suggesting merits of open source exploitation. In the absence of any useful way to compare relative contribution between the intelligence disciplines, the denial culture that sees closed as more useful than open remains the norm. Arguably, in a single source practice the decision to incorporate open source exploitation enterprise-wide is less

threatening and less complicated than the incorporation of competing closed intelligence disciplines.

Thus, in the all-source examples (DIS, EUROPOL, SOCOM) open source exploitation sits figuratively alongside the more established closed collection sources (Humint, Techint, Masint) as input to the all-source intelligence process. However, unlike the output from the supplying agencies, which reside outside the customer agency, these OSINT cells sit inside, 'bolted-on' to the analysis effort (see Figure 4.4 below). Arguably, they have an inside track that should give them an advantageous position from which to 'sell' their effort, yet often they cannot, as in the DIS case, and, so demonstrably by 2006, the EUROPOL case. These structural and cultural issues are interesting and discussed further in Chapter Five.

Figure 4.4: All-source OSINT treatment model

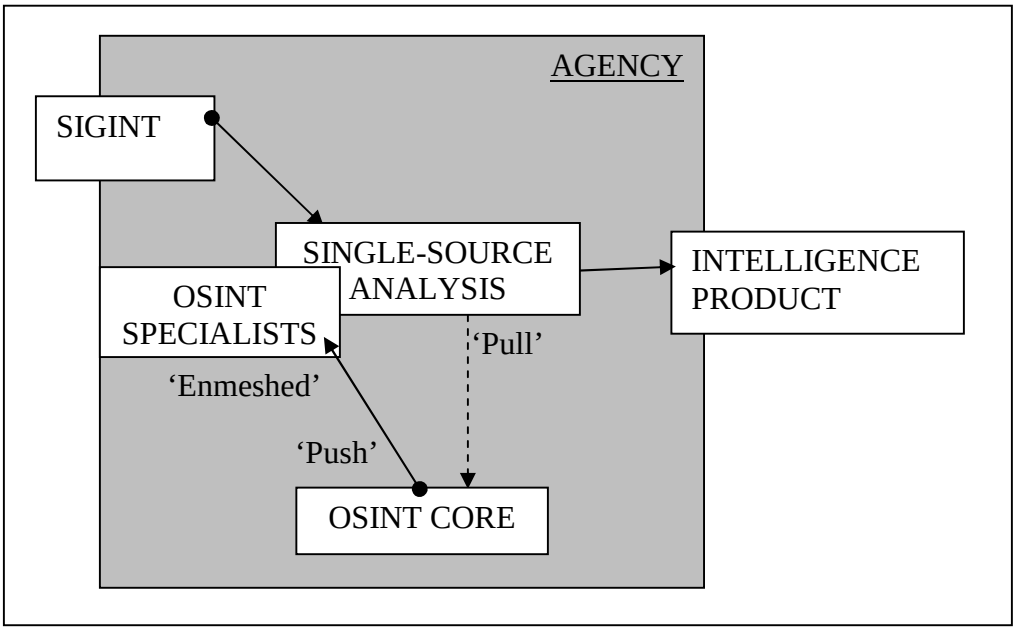


Source: Author

In the single source agencies, OSINT exploitation is not so clearly defined as a discrete input to analysis, where information is collected from or 'pulled out' of a unique location.

Rather it is 'pushed out' to desk officers/analysts wherever they are and merged as seamlessly as possible with closed sources. This variation in placing has a secondary effect upon the style of OSINT delivery, which additionally helps categorise OSINT exploitation. All source agencies, where OSINT exploitation tends to be discretely centralised, generates a broadly pull approach from its customers. Whereas, single source agencies, in which OSINT exploitation is more distributed, generate a broadly push endeavour to their customers. Having said that, they also maintain a central pool of open source expertise that analysts can return to for additional help or resource; but it is not the front line of the activity (see Figure 4.5 below). Again, this is interesting, and perhaps not surprising given the intellectual locus of the UK's OSJWG, that it reflects the national policy direction of both the UK and US to centralise open source expertise into a professional discipline at the centre while maintaining professional practice as far away from the centre and at the cutting edge of intelligence work as possible. This is probably best represented by the US OSC's expressed intention to be the co-ordinating core for a national community-wide virtual open source collaborative effort.[107]

Figure 4.5: Single-source OSINT treatment model



Source: Author

Exploitation - collection, or analysis, or both

Regardless of the agency and its treatment of open sources of information, there is no doubt that they all engage in it. Because of the lack of clear demarcation between collection and analysis of open sources, more clearly observed in the other intelligence disciplines, the term open source exploitation is used in preference to simply collection. Indeed, the US has coined the term 'open source enterprise' to cover the activity.[108] It is a moot point, whether the product of the OSINT cell is merely collected data or analysed information. In all the public sector intelligence agencies examined the product of open source exploitation goes to analysts for further treatment. One man's output is another man's input so to speak. However, this initial exploitation certainly incorporates varying degrees of selection, filtering, and choice by the OSINT cell. It is certainly interpreted to some degree or another.

Thus, four observations emerge from an initial exploration of the treatment of OSINT within these agencies:

- All the intelligence agencies conduct open source exploitation. This either suggests that they consider it useful or they simply do it because they can. There is no obvious metric that compares the relative use of one 'int' against another.
- Broadly, the originating OSINT effort in all the agencies is heavily collection oriented. Certainly, the OSINT cells conduct no ***formal*** analysis of what they collect into what might be understood as final or evaluated intelligence product. Even the ASD product is heavily qualified before going forward to final intelligence product.
- Within the agencies the collection of OSINT ranges from being virtually indistinguishable from closed sources to a separate discrete operation. There is either no national best practice or no best practice suitable for bespoke operations.
- Institutionally, open source product does not have the same gravitas or weight associated with that derived clandestinely, yet individually, it is hard to find a senior intelligence professional who would articulate that view today.

Suffice to say at this point that within private sector information brokerages (PIB) the same 'unit' if not the same person often undertake both collection and analysis. This occurs mainly because PIBs are relatively small in comparison to public sector intelligence agencies (an efficiency requirement) and because each member of staff has both collection and analysis expertise (an effectiveness argument). However, it is interesting to note that as a PIB expands organisational dynamics tend to force them to separate out collection from analysis and some additional quality control audit has to be put in place before product is released.[109]

The exploitation of open source seems stuck in a position where its efficiency is understood, often measured for effectiveness, but only against itself and therefore not evaluated for efficacy against other intelligence disciplines or against wider objectives. In the absence of these strategies it cannot easily be supported by a corresponding allocation of additional resource or the re-distribution of existing resource. It seems in a state of limbo. Where metrics are used to measure performance they are done reflexively to justify their own position rather than comparatively to facilitate broader resource allocation across the intelligence disciplines.

Effectiveness and policy

Two further observations stand out in this initial understanding of OSINT's place within the intelligence community. First, it remains difficult to evaluate the effectiveness of OSINT exploitation. Beyond a simple counting of the number of 'calls' upon the OSINT cell, together with some qualitative assessment of the customer's view of its usefulness, there is little uniform or meaningful assessment of the efficacy of OSINT. Arguably, this is also the case for the broader intelligence function. Second, there is little national policy or strategy with regard to the exploitation of OSINT. It has by and large evolved agency by agency. Both seem important and connected.

At an operational level in the UK, a coordinating body for OSINT exploitation - the Open Source Joint Working Group (OSJWG) - has been established since 2000. Yet, there has

been little direction from the national level - 'top down' - until hitherto. Only recently has there been connection made between national and agency approaches through the appointment of a national 'open source champion' in late 2005. This appointment provides a conduit between Cabinet level bodies, notably the JIC and Permanent Secretary (Intelligence, Security and Resilience) and the Intelligence Community for open source matters. Interestingly, this appointment is combined in one person with the responsibility for the professionalising of analysis under the title 'Professional Head of Analysis'. The responsibility for developing policy, doctrine, training and standards thus resides with the OSJWG, a devolved, semi-permanent committee of open source experts, who meet infrequently and have other full-time professional engagements to fulfil.

Conversely, in the US much has been made of the November 2005 appointment of an Assistant DNI for Open Sources (ADDNI/OS) together with the establishment of an Open Source Centre located within the CIA. Additionally, direction of a National Open Source Enterprise (NOSE) led by the ADDNI/OS in conjunction with an advisory board to be constituted from government and non-government representation has been stipulated in Intelligence Community Directive 301 of July 2006.[110] Thus, the national open source endeavour in terms of policy, standards, training, and doctrine amongst other matters is still emerging in the US. However, the locus of the endeavour is being crystallised into a permanent body. Whether its position, firmly under the purview of the CIA for budgetary matters with recourse to 'top cover' from the DNI, is practically workable remains to be seen.

It might tentatively be posited that the measurement of effectiveness and national open source policy form a vicious circle. Without some understanding of OSINT's value, there is little reason to effect change beyond intuitive reasoning. Obviously, it would be beneficial to measure the contribution of OSINT in comparison to the clandestine intelligence disciplines as this might help determine its appropriate 'weighting' in the intelligence function. However, other than some incorporation of 'soft' evaluation measurement, there is no apparent quantitative measure of intelligence effectiveness and

thus no best way to allocate tasking holistically across the intelligence disciplines rather than arbitrarily within them.

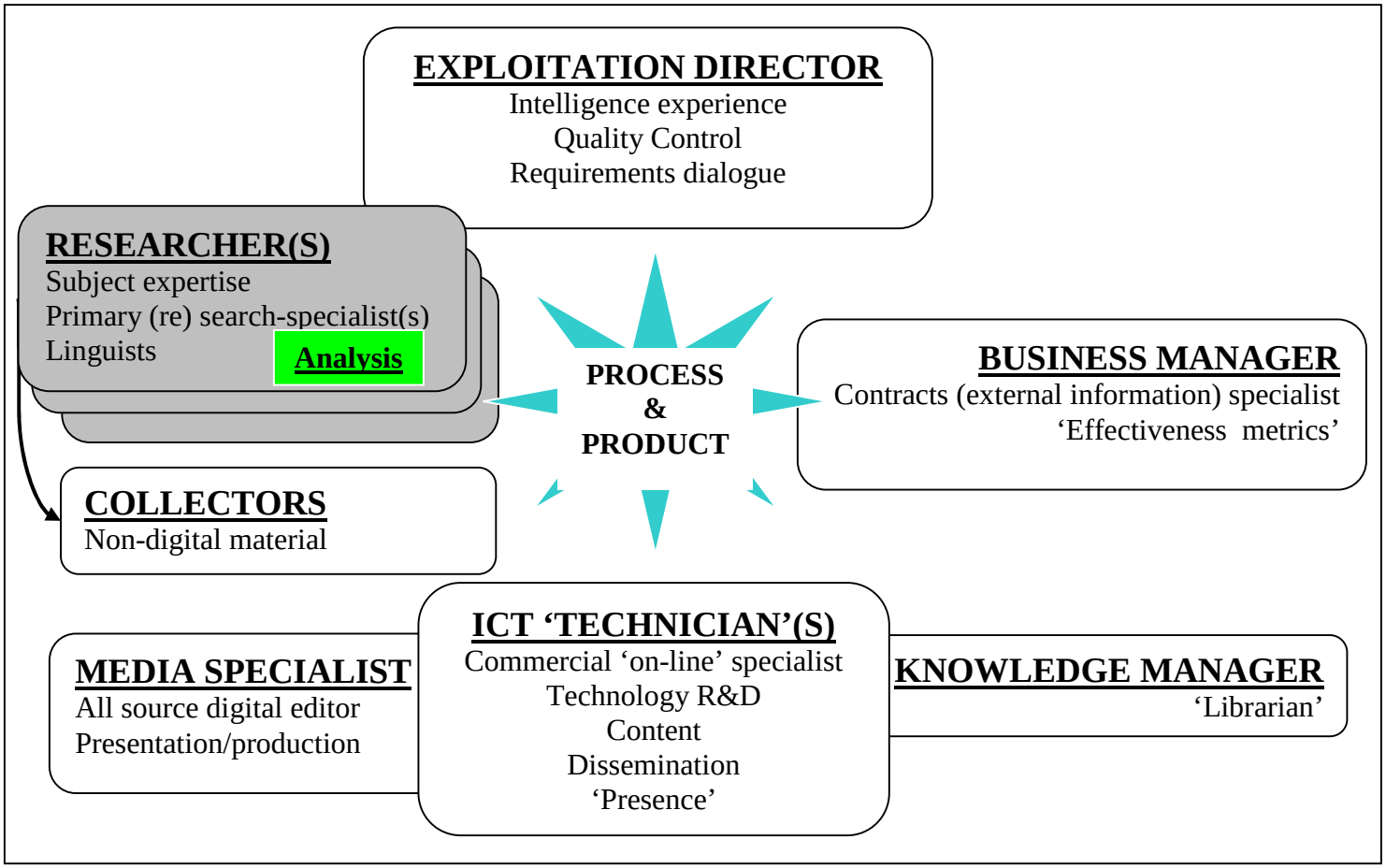
What has been observed in one of the studies (OSJWG), and discussed further in the analysis, is a recognition that OSINT can act as cross-check for the closed intelligence product of the clandestine agencies; and in so doing offers a measure of the effectiveness of closed collection against what is known from open means. It seems that such a measure can only be known within the agencies themselves and even then with some considerable and 'senior' effort. It is unlikely to be open for examination by any independent external source. The obvious data collection point and ultimate arbiter of effectiveness probably resides with the customer.[111]

4.4.2 Typical OSINT exploitation structure

The exploitation of OSINT, regardless of its process (push to pull) or place (central to dispersed) necessitates some fundamental functions that are expressed across all the organisations investigated to one degree or another. Collectively, they might form a useful generic structure of 'must-haves' for effective open source exploitation. Indeed, the majority are familiar to any intelligence operation and reflect the intelligence cycle. Even more broadly, they reflect decision-making cycles and a systems approach common to many organisations, which necessitates balancing inputs, outputs, process and constraints. At one extreme, private information brokers (PIBs) carry out all these functions in one person. At another extreme, the National Co-ordinating Unit (NCU) at HMRC has an 80-strong staff conducting the collection element alone. Open source exploitation variously maximises some of the functions and minimises others.

Figure 4.7 displays a generic OSINT cell structure based upon common and necessary functions for open source exploitation. This has been derived from triangulating the literature with the organisations visited. It is worth emphasising that this structure does not necessarily exist in a single case-study, although the ASD structure comes close (compare Figures 4.6 below and 4.2 above).

Figure 4.6: Generic model of an OSINT cell



Source: Author

Common OSINT Exploitation Elements

The following critical elements seem crucial to OSINT exploitation:

- **Researchers and Cell Directors.** Researchers, variously called information specialists or search specialists in OSINT exploitation, and cell directors seem entirely compatible with any intelligence organisation. However, by virtue of the global provenance of open sources, it is crucial that researchers have linguistic, cultural and technical expertise pertinent to their target areas. The cell directors have increasing

responsibility for quality control as their cells have increasing responsibility for the interpretation (limited or otherwise) of their information before further dissemination.

- **Business Manager.** Equally, most intelligence organisations require a financial function. However, in the case of open source exploitation, given that open sources of data or analysis are invariably not free, and, given that their supply needs 'maintenance', it seems important enough to some open source organisations to have a contracts manager in place.
- **ICT Technician and digital presentation.** Additionally, given the high dependency on ICT tools and techniques, it also seems sufficiently important for OSINT cells to have some permanently available ICT expertise, whose role is again one of maintenance, as well as keeping a watching brief on emerging and useful technologies. The final stage of the intelligence cycle requires a need to produce and present information for dissemination to customers. Inevitably, this function has an increasing digital content and Internet presence.
- **Knowledge Manager.** The shear volume of data, information and finished product that all organisations produce demands that storage at least and timely access at best is considered. The famous Rumsfeld quote about known knowns and unknown unknowns, which in this author's view was rather too quickly denigrated, probably also sums up the information conundrum for all organisations and certainly intelligence ones.[112] Indeed, the director of intelligence analysis at HMRC mentioned that organisationally: "Knowing what we already know ourselves is a considerable challenge."[113] Knowledge management was only formally treated by two of the initial cases (the OSJWG agencies certainly and HMRC to a degree) and conducted organisation-wide rather than specifically for open source exploitation.[114] The management of knowledge as precursor for doing something useful with it is an emerging requirement of all organisations. Yet, this 'new' requirement is something librarians have been doing for years.[115] The management of information or knowledge seems a useful function of the open source cell; but it is not yet clearly delineated.

Organisational dynamics

In some organisations, the early days of OSINT exploitation are characterised by many of the common functions, certainly the three functions of research, ICT 'savvy', and information dissemination, residing in just one or two individuals. In time, as customers increase, as requirements increase, and as products increase, these procedural functions tend to separate out as a result of simple external commercial (demand) and internal organisational (supply) pressures. Both HMS and Exclusive Analysis went through that process in 2004/2005. BBC Monitoring, established on the eve of World War II, represents the latest iteration of organisational structure as the largest and oldest example of an agency devoted solely to open source exploitation. In order to ensure the best possible service to its customers, BBC(M) has established an extra function not specifically identified elsewhere - a customer relations function. Their Business Development and Customer Relations team handles stakeholder, commercial business, and partnership relations and includes account managers, who work with the respective stakeholders. Similarly, their stakeholders have respective 'partner' bodies, which work with them. As a quasi-public sector organisation largely sponsored by government departments they also demonstrate organisational structure fashioned by constraints, notably a set budget determining their resource allocation.

Structure and analysis

The issue of analysis comes up again in regard to deliberate organisational structure. Public sector agencies, as has already been mentioned, appoint no designated formal analysis posts or functions within the open source organisation, whereas, in private sector organisations it is *de rigueur*. In PIBs, while the functions in the model above seem inexorably to divide out, the division of research and analysis does not. Research and analysis reside in one individual in the early phases of establishing an open source effort. The only difference between individuals is experience and effectiveness.

Thus, it is worth emphasising that, in the private sector, search-specialists are not people who simply know how and where to look; but are also people who know something about what they are looking for. They bring subject matter expertise and are capable of analysis

in their own right. However, it would not be true to say that analysts are necessarily good information specialists. They have had to learn the search and research techniques appropriate to the digital age that their equivalent public sector organisations usually begin with as information specialists or librarians. There is one interesting anomaly - the UK Foreign Office Research and Analysis Division, a public sector organisation, where, as the name suggests, employees are expected to undertake both research and analysis.

Thus, broadly, the public sector organisations tend to retain search specialists in the narrower requirement avoiding analysis for which there is a separate cadre, while the private sector tends to combine both. This distinction between strict job description and broad flexibility emerged continuously throughout the research. It seems to represent a crucial difference between public and private sector open source exploitation and is treated further in the discussion and conclusion.

Suffice to say at this point that the research begins to discern 'passive' from 'active' exploitation, reflecting an imbalance between the 'location' and 'separation' of analysis and collection. How much more effective might PIB analysis be if their collection effort was enhanced by closed information? How might intelligence product change if closed source were reversed out to PIBs? In some cases, where the expertise is apparent, this is already being mooted.[116] The danger might be that this arrangement plays into the hands of one of Butler's bear-traps, namely that 'groupthink' is (re) established by the very effort of trying to encourage 'red-teaming'. Similarly, how much more value could be added if the collection expertise of public sector open source cells was enhanced by subject matter expertise? Nowhere is this more clearly exemplified than at BBC monitoring, where subject matter experts merely collect, at least at a formal level, and are discouraged from intelligence analysis albeit conducting a specialised media analysis. It seems so wasteful.

Structure and Reform

In open source exploitation, at least in the private sector, the so-called 'reform' advocated in some of the literature is already being practised. A key thrust of Berkowitz, and

supported by Hulnick, is the notion that there is too much separation between collector and analyst and analyst and policy-maker.[117] For PIBs commercial necessity and bureaucratic agility tend to find collector and analyst rolled into one person together with a very short link to policy-makers. HMS explicitly states the imperative for combining research and analysis: "I could not do my job without knowing the facts and keeping up to date with them."[118] The implication that analyst-policy-maker contact is crucial is implicit. The separation of collection and analysis has simply not arisen in the post Cold War, global, ICT-rich PIBs of the last 15 years. However, the legacy structures and culture of the truly secret intelligence Cold War, that necessitated compartmentalisation, is still perpetuated to some degree in the public sector, contrary to the contemporary need to share information; the absence of which may aggravate security risks rather than diminish them.[119]

There are efforts to redress the segregation *between* analysts at least.[120] Terrorism and proliferation have seen 'joint centres' or 'fusion centres' being established, where analysts from the various agencies are forced together. The National Counter-Terrorism Center (out of the Terrorist Threat Integration Center) and the National Counterproliferation Center, both established under the DNI in the US in 2005, and the Joint Terrorism Analysis Centre and Serious Organised Crime Agency established in the UK are just a few examples of this cooperation; but it does not necessarily represent a union of collection and analysis. Furthermore, while the analysts may come together, they also import with them new versions of the fundamental issue of security that impinge upon sharing. As has been mentioned, PIBs find that as they grow, they become susceptible to the challenges of organisational growth (although some like PRA express a clear desire not to grow for this reason) and, while evidence has not been found in this research, may be similarly compelled to separate out collection from analysis. Hulnick argues that the cultural and institutional change required to reverse this situation must come from the top down rather than the bottom up.[121] This author suggests that real and meaningful change can also occur from the bottom up, but is as likely to be suppressed by those at the top. The DIS and UK JTAC demonstrate this to differing degrees.

4.4.3 Aggregating and 'naming' the high order benefits

The data collected from the case-studies have demonstrated the high order benefits peculiar to the exploitation of OSINT. It would be incorrect to suggest that these benefits are exclusive to open source exploitation alone. However, they are more representative of the contribution of open source exploitation than closed. Open source exploitation is where the intelligence function would go first to generate these contributions rather than closed. Given the way in which the contemporary debate on intelligence is often framed - polarised as open versus closed - it seems inevitable that they are observed in comparison. However, it is worth re-emphasising the author's intention to understand how open source exploitation contributes to the intelligence function rather than how it competes with the other intelligence disciplines.

Thus, the specific benefits and peculiar contribution of open source exploitation are aggregated and re-stated here as high-order factors that best describe the contribution of OSINT to the intelligence function:

- **Context**

  Without exception, and as 'advertised' in the literature, the case-studies all recognised that open sources of information represented a 'matrix' in which, or upon which, to conduct their work; described variously as 'a first port of call', 'stocking filler', 'background', 'the landscape in within which the classified features sit', 'a basic grounding', or simply 'contextual material'. This feature of open source is the most widely acclaimed. There was little distinction between context, that which surrounds the subject of interest and taken here to mean background information, and *contextere* as in to weave together or taken here to mean sense-making through connection.

- **Utility**

Utility was often mentioned as synonym for speed, volume, and cost. It is considered quicker, more productive, and cheaper to exploit open sources of information than closed. Thus, it is more immediately useful to analysts. However, utility is also observed to pertain to a notion of 'value-added'; a sense that the information derived from open source exploitation actually creates value or utility for the customer. That it can be 'used' is a benefit in its own right. This was mentioned frequently by both public sector analysts and commercial private information brokers. It is not surprising that the latter group might claim usability since it provides them with livelihood; but the tone of the comments of the former were genuinely meant rather than cynical, and in contrast to much of their previous experience inside the traditional intelligence community.[122] This in itself reveals the 'spies only know secrets' mantra advocated by Steele.

Arguably, the element of usability precedes and stimulates the notion of communicability - the sharing of information. Thus, this aspect of utility seems to straddle both utility and communicability for the time being in this thesis.

Finally, in the utility bracket, is the notion of hazard. This feature emerged from discussion among senior intelligence practitioners within the Oxford Intelligence Group (OIG) and was precisely articulated in a discussion on the ethics of intelligence in October 2006. One aspect of the utility of open source is that its exploitation should broadly entail a lower risk than other generic sources. In particular, and attractively so to the OIG, was the lower moral and ethical hazard that open source carries. Furthermore, its exploitation removes unnecessary hazard, including moral, that is automatically charged to closed, clandestine, or secret intelligence methods.

- **Crosscheck (Benchmark)**

  The emphasis on this factor came from the very strong advocacy of OSINT as cross-check by OSJWG single agency and Cabinet Office practitioners; but was not specifically 'advertised' as a benefit anywhere else. However, it matched the more

reform-oriented literature on intelligence. The important point made by the interviews is that open is as much a crosscheck for closed as closed is for open. Whether this two-way street is equally balanced seems worthy of further investigation.

- **Focus**

  Focus connotes direction as well as acuity. Acuity in the context of intelligence suggests the depth to which a subject is examined or the granularity which is revealed by examination. Direction suggests the targeting onto another subject as a result of examination; an alternative 'lead'. Thus focus here has two meanings - depth and direction. The ability of open source intelligence to focus or 'direct' closed sources as in point them more acutely is highly acclaimed in the literature; but not so uniformly observed in practice. Clearly where private information brokerages are concerned, their access to closed sources is severely restricted. Nevertheless, it is apparent that informal relationships between closed agencies and private brokerages channel communication between them. In the case of Hazard Management Solutions (HMS) closed agencies are actively pursuing how to reverse out their closed information to be analysed where the expertise resides. This might actually represent the reverse of what the literature suggests. Rather than the closed being put on to the scent by the open, the open is being directed by the closed. A variety of explanations might explain this phenomenon from seeking open source to aid communication of what is known clandestinely to lack of resource to lack of expertise. In the HMS case, it seems clear from an examination of staff experience and client list that the expertise is exceptionally strong. In this particular and highly specialised instance the extreme benefits of open source exploitation are revealed - the redundancy of the closed collection. Open source collection does not merely (re) direct and/or 'narrow' closed collection; but implicitly takes it over in a controlling sense.

- **Surge**

  Clandestine intelligence, particularly Humint, is not an activity that can be turned on and off like a tap. Conversely open source information, which is already 'out there',

distributed, and reflecting an amalgam of all closed intelligence disciplines is more easily manoeuvrable to new targets and requirements than the traditional sources. In this regard it can fulfil a surge capability in demanding times - times of crisis - until closed means are brought to bear.

- **Communicability**

  One of the constantly repeating themes of the intelligence enquiries of 2004 was the inability of intelligence agencies to share information with each other, and their respective governments to communicate risk to their publics. The notion of security is often cited as rationale for an inability to share, whereas issues of bureaucracy, technology, culture, and politics are equally complicit. Indeed the Federation of American Scientists has uncovered several 'papers' that point to increasing insecurity as a result of not sharing.[123] Theoretically, it should be increasingly possible to share information that is derived from open sources given that it is legally available in the public domain. The security aspect then shrinks to who collects it rather than who from. Whether open source will punch through the cultural, institutional and political barriers to sharing remains to be seen. Communicability was also referred to as 'usability' and thus connotes notions of utility too as discussed above.

- **Analysis**

  Information is the precursor to analysis. Analysis broadly comprises five varieties, each of which is variously undertaken by open source organisations:

  - Current intelligence in order to maintain information on developments of current crises, events and situations.
  - Database or knowledge creation in order to surge capacity for future events.
  - Forecasts that estimate future developments.
  - Warnings and indicators in order to alert that a crisis is looming or begun.
  - 'Red Teaming' in order to question existing analysis, its assumptions and conclusions based upon alternative information sets and/or alternative analysts.

> The open source cell within the intelligence branch of the UK's Joint War Headquarters is specifically charged to offer alternative analysis based upon open source exploitation.[124]

The degree to which the collectors of open source undertake analysis varies considerably. All the cases conduct filtering, processing and presentation of information at the very least. The issue is not whether open source information provides material for further analysis; but who does it. Open sources of information are no more or no less susceptible to the required virtues of all information, however derived.

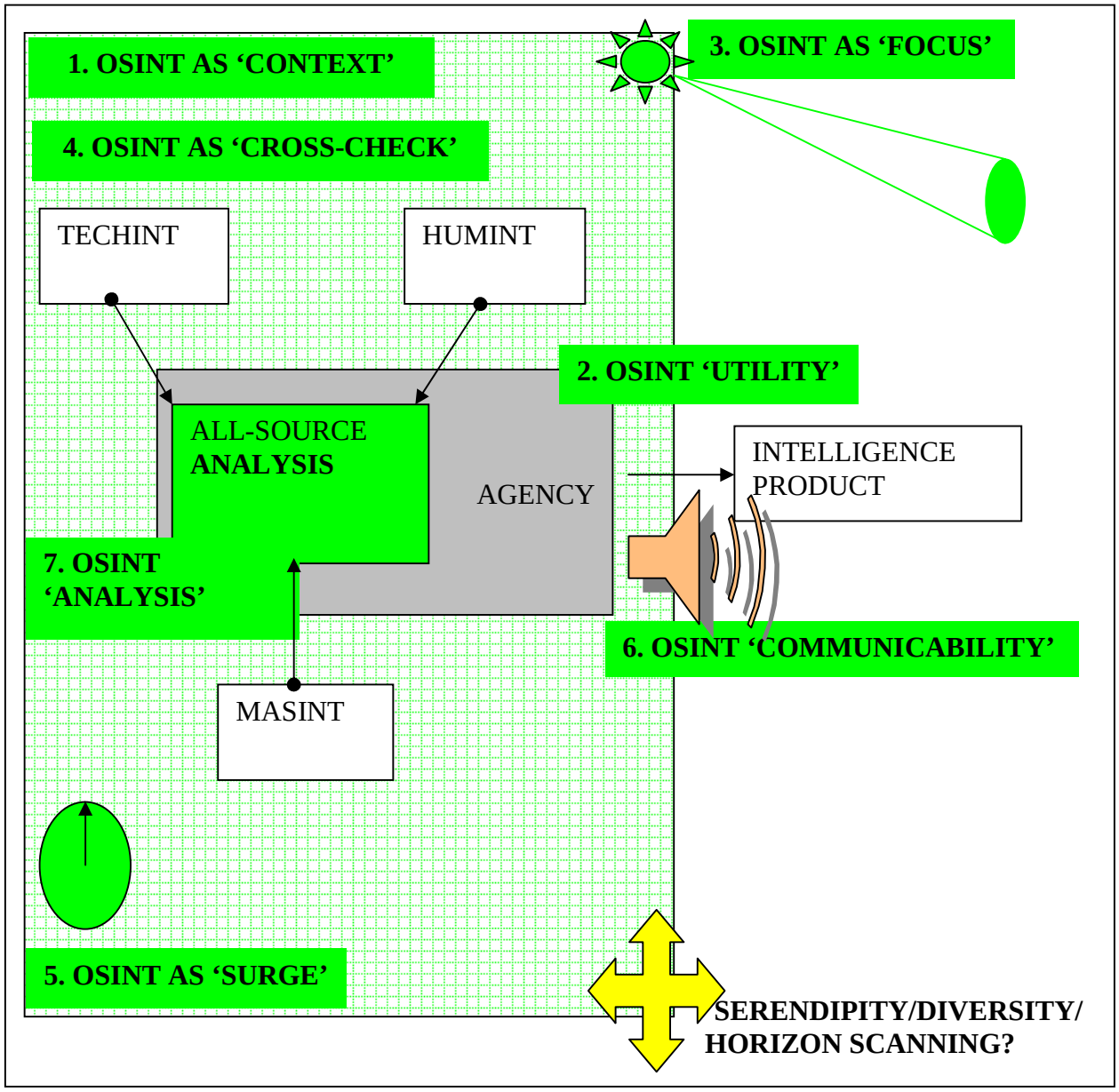
In private information brokerages, collection and analysis, for that matter the entire intelligence cycle, is undertaken by individuals, or groups of individuals comfortably interchanging between all elements of the cycle in order to create product. In public sector agencies, analysis seems entrenched with those designated as analysts. The ICTY and BBC Monitoring present 'halfway houses'; yet, crystallise the differentiating factors that determine who does analysis - expertise and necessity.

It is equally pertinent to note that OSINT also contributes significantly to 'counter-analysis' or 'red-teaming'. It is particularly useful in this regard because it can present a separate data set alongside that of closed sources. In the absence of an alternative data set only the analysts can be varied. With open source both the data and the analysts can be varied and the latter from outside a community that might tend toward the heuristic of groupthink.

These high order factors might usefully be represented as an overlay to the location of open source exploitation (see Figure 4.7 below). Additionally, the notions of serendipity, horizon-scanning (first alert), and diversity are noted because they are explicitly used by senior open source practitioners within intelligence communities. However, they do not uniquely describe the contribution of open source intelligence, or are better subsumed into

the factors described above. It is certainly possible that 'golden nuggets' can emerge by luck from open source exploitation and maybe more so than from closed, but closed can also be serendipitous or capable of spotting some far-off risk.

Figure 4.7 The seven High Order Factors



Source: Author

The notion of 'diversity' is interesting, not least because a very senior open source practitioner advocates it as underpinning rationale for the exploitation of open source.[125] The diversity of open source in terms of being able to offer different 'views', assessments, or analysis is an extremely valid claim that has given much cause for thought. On balance it is considered too broad a descriptor for open source as it can imply much more than diverse analysis, and thus everything and nothing at once. For example ideas emerging as a result of social computing: 'swarming'; the 'blogosphere'; 'the wisdom of crowds'; or 'an army of Davids', can allow 'work' to be shared out across the intelligence commons rather than merely within the intelligence community.[126] The US DNI engaged in such an effort following the release of captured Iraqi documents to the World Wide Web in early 2006.[127] Such notions of collective or distributed intelligence are increasingly apparent, although as the search for extraterrestrial life (SETI) shows, again, not new. But, this diversity might equally convey, implicitly if not explicitly, 'context', 'utility' and 'focus', as well as 'analysis' in the sense of 'red-teaming' or countering 'groupthink'. Thus, because it is too broad a description it is discounted for the purposes of this model. It is a very useful metaphor for open source exploitation, but it does not accurately pin down its contribution.

4.5 Summary

This chapter has built upon the literature's partial understanding of OSINT's contribution to intelligence. It records the extraction of data from a series of case-study organisations, conducting the exploitation of open sources of information as part of a broader intelligence function. This additional and more discerning data were obtained by semi-structured interview with producers, customers, and policy directors of open source exploitation as well as participant observation within target organisations. It has been collected, laid out, and triangulated from the bottom up into a set of high order factors that describe the contribution of open source exploitation to the broader intelligence function. The model constructed in this chapter identifies seven such high order factors: context; utility; focus; surge; cross-check; communicability; and analysis.

Additional observations were also made on the generic structures and processes of open source exploitation cells. Thus, the research begins to describe the structure, process and development of open source exploitation within intelligence organisations and as part of the intelligence function.

The next chapter analyses the results of this data collection both for the contribution they make to an understanding of open source exploitation as well as the impact for intelligence as a whole. Suffice to say, at this point, that these high order factors are only useful to the internal policy, direction, and resource allocation of the intelligence community itself. There is no apparently obvious way of measuring the effectiveness of intelligence as a whole to society, let alone the specific effectiveness of open source exploitation. Thus these high order factors are only relevant, in terms of effectiveness, internally within the intelligence function. Yet, even internally there is no apparent effort to determine relative effectiveness across the various intelligence disciplines or agencies beyond what the customer or consumer decides. Looking at the intelligence function as a whole, but from an external position, the effectiveness debate becomes one of efficiency and thus one of where best to allocate resource. Either way, the discussion dissolves to the thorny issue of the allocation of resource to open source exploitation, either relatively to other cost centres within the intelligence community if resources are fixed, or absolutely if resource were to suddenly become unlimited. Part of that discussion must include an understanding of exactly how open source is recognised to contribute.

Notwithstanding the establishment of the OSJWG in 2000, the OSC in 2005, intelligence community open source champions in 2005,[128] and a continuation of intelligence inquiries from Franks to Butler and Dulles to Silberman and Robb that argue the case for increased open source attention,[129] the exploitation of OSINT in the UK and US, at least, has evolved piecemeal. This has partly been due to the normal compartmentalisation and stove-piping of agencies that characterises intelligence communities: partly because of a broad cultural antipathy to open source exploitation that has, hitherto, seen it as ‘inferior’ (perversely

because it is perceived cheaper and less difficult to collect and thus less ‘sexy’); and partly because open source practitioners do not carry any collective ‘clout’ to effect change. In the US, the creation of the DNI Open Source Centre in November 2005 signified recognition of open source exploitation at the highest level. These respective approaches – procedural versus structural - simply reflect the different culture, traditions and resource of both intelligence communities rather than any inherent recognition of the effectiveness of OSINT.[130]

References and Notes:

[1] Gannon, J.C., 2000, Address to the Washington College of Law at American University Washington DC, 6th October, 2000.

[2] Interview, 2003, EUROPOL 6, Den Haag, 16-18 April 2003.

[3] Interview, 2005, DIS ANON R1, London, 20 October 2005.

[4] BBC-M 1, ongoing conversation 2002-2006.

[5] Interview, SOCOM 1, MacDill AFB, Tampa (FL), 18-20 April 2006; Interview, 2007, ASD 1, 29 January-2 February 2007.

[6] Review of BBC Monitoring, 2005, p.4, as cited in: UK Intelligence and Security Committee, (Ed) 2006, *Annual Report 2005-2006*, Cm 6864, p.26.

[7] A useful summary of how they are perceived from an intelligence perspective can be found at: UK Intelligence and Security Committee, (Ed) 2006, *Annual Report 2005-2006*, Cm 6864, pp.26-27.

[8] BBC Monitoring, 2007, *A Year in Review 2006/2007: The World in its own Words*, July 2007, available at: http://www.monitor.bbc.co.uk/review.pdf

[9] As noted in Chapter One (1.8), the creation of the US DNI's Open Source Center at the CIA on 1 November 2005 saw FBIS being absorbed into its organisation.

[10] Presentation by Director BBC Monitoring to Oxford Intelligence Group during visit to BBC Monitoring, Reading, 17 May 2005.

[11] BBC Monitoring, 2007, A Year in Review 2006/2007, *op cit*, pp.16-17. In 2003, BBC Monitoring's funding was £20.215m from these four stakeholders with an additional £5.716m from other income, of which £1.627m came from commercial sales. See BBC Monitoring pamphlet: BBC Monitoring 2003-2006 dated July 2003, available at: http://www.monitor.bbc.co.uk/corp_plan2003.pdf This budget was raised slightly in 2005 for an agreed reduction in staff levels.

[12] Foreign and Commonwealth Annual Report 2004-05, 15 February 2006, pp.60-63, available at: http://www.publications.parliament.uk/pa/cm200506/cmselect/cmfaff/522/522.pdf The figures cited on pp.61-62 are now out of date.

[13] Private correspondence with BBC Monitoring.

[14] *Ibid.*

[15] Goss, P., 2004, *DCI Goss Addresses Employees*, available at: http://www.fas.org/irp/cia/product/goss092404.pdf

[16] *Ibid.*

[17] Hillson, D., Murray-Webster, R., 2005, *Understanding and Managing Risk Attitude*, Aldershot: Gower Publishing; Slovic, P., 2000, *The Perception of Risk*, London: Earthscan.

[18] Presentation by Director BBC Monitoring to Oxford Intelligence Group during visit to BBC Monitoring, Reading, 17 May 2005.

[19] Foreign and Commonwealth Annual Report 2004-05, *op cit*, p.60.

[20] BBC Monitoring, 2007, A Year in Review 2006/2007, *op cit*, pp.7 & 10-11.

[21] Best, R.A., (Ed) 2006, *Intelligence Issues for Congress*, Washington: US Congressional Research Service, Report No: RL 33539, p.6.

[22] Goss, P., 2004, *op cit*, p.4.

[23] The National High Tech Crime Unit was disbanded and some parts absorbed into the Serious and Organised Crime Agency during 2005/2006.

[24] Nor can 'closed'. Apocryphally, point intelligence comes round only every 8 years or so.

[25] The IAEA work on nuclear weapons proliferation is virtually all open source; anti-globalisation and animal rights activism can be tracked openly; counter-terrorist intelligence is strongly supported by OSINT exploitation; much policing work is achieved using open source data bases.

[26] Renier, O., Rubinstein, V., 1986, *Assigned to Listen: The Evesham Experience 1939-1943*, London: BBC Books.

[27] Private correspondence with BBC Monitoring, 13 July 2007.

[28] BBC Monitoring, 2007, A Year in Review 2006/2007, *op cit*, pp.6-7.

[29] Private conversation with Director OSINT exploitation US SOCOM.

[30] The Global War on Terror has become a contentious descriptor. In 2006, it could be seen that both the US and UK were keen to distance themselves somewhat from it. For example, CENTCOM referred to it as the 'Long War', while on the same base SOCOM continued to call it GWOT, during my visit there in 2006. In 2007, it became apparent that both terms were being abandoned as their implied longevity ran counter to talk of withdrawal and drwdown.

[31] Presentation to OSS Conference, November 2003, Washington DC.

[32] See Chapter Five, Sections 5.1.2, 5.1.4, and 5.2.4

[33] Private correspondence with UK Defence Academy's Conflict Studies Research Centre.

[34] This is supported by the 2005/2006 DIS review of open source exploitation discussed in more detail in section 4.2.5.

[35] There have been 2 Presidential Directives issued to this effect: Press Directive 2004/5. Of course, 'imposed' does not necessarily mean undertaken.

[36] Private correspondence with two agencies.

[37] 108th Congress Report to Senate (2nd Session) 108-258. May 5, 2004, available at: http://www.fas.org/irp/congress/2004_rpt/s108-258.html

[38] Intelligence and Security Committee, (Ed) 2006, *Annual Report 2005-2006*, Cm 6864, pp.24-26.

[39] Interview, 2005, DIS Anon R1, London, 20 October 2005.

[40] Interview, 2005, DIS Anon R2, Shrivenham, 28 October 2005.

[41] Available at: http://www.oss.net/extra/news/?module_instance=1&id=1334

[42] Gibson, S.D., 1997, *The Last Mission Behind the Iron Curtain*, Stroud: Sutton.

[43] Conversation with a former SIS employee at an Oxford Intelligence Group meeting.

[44] Hulnick, A.S., 2004, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Westport, CT: Praeger, p.xii.

[45] Interview, 2005, PIB 1, UK, 7 September 2005.

[46] See: www.hazmansol.com for examples

[47] See Allen-Vanguard press release, available at: http://www.pr-inside.com/allen-vanguard-announces-agreement-to-r98303.htm

[48] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis.

[49] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, p.2.

[50] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.22, 28-31, 48-50, 101.

[51] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, p.101.

[52] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.6-12.

[53] BBC News Online, 2004, 'London Terror Attack Inevitable', 16 March 2004, available at: http://news.bbc.co.uk/1/hi/uk_politics/3515312.stm

[54] "The Threats", MI5 (British Security Service) website, produced in October 2005, available at: http://www.mi5.gov.uk/output/Page23.html

[55] Interestingly, HMS made a similar forecast in March 2001 to the BBC 48 hours prior to the White City taxi bomb on 3 March of that year.

[56] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, p.2.

[57] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.23-24, 102-106.

[58] North Korea is barely analysed in the report, suffice to say that there will be less willingness to talk to North Korea as their progress to a nuclear capability continues (*Ibid*, p.23). It remains a most impenetrable, secret state, more susceptible to secret intelligence gathering than open source exploitation. However, the subsequent case-study of the ASD demonstrates that penetration of North Korea using open source exploitation is highly valued.

[59] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.23-24.

[60] Report of the International Independent Investigations Commission Established Pursuant to Security Council Resolution 1595 (2005) dated 19 October 2005, available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/21_10_05_mehlisreport.pdf

[61] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, p.24. The report refers to 'Mukhabarat', which is the generic Arabic word for intelligence (agency implied), but does not specifically say which of Syria's three main intelligence agencies.

[62] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, p.24.

[63] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.117-118.

[64] BBC News Online, 2005, 'Saudis Vow Loyalty to New Monarch', 3 August 2005, available at: http://news.bbc.co.uk/1/hi/world/middle_east/4740741.stm

[65] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.113-119.

[66] Exclusive Analysis, (Ed) 2004, *Global Risk Outlook 2005*, London: Exclusive Analysis, pp.118-119.

[67] Friedman, G., 2004, *America's Secret War: Inside the Hidden Worldwide Struggle Between the United States and its Enemies*, London: Doubleday, Random House.

[68] Hillson, D., Murray-Webster, R., 2005, *Understanding and Managing Risk Attitude*, Aldershot: Gower Publishing.

[69] HMS monthly Triton Reports 2003-2004 held with the author.

[70] Interview, 2005, PIB 1, UK, 7 September 2005.

[71] Interviews, 2005, DIS ANON R1, London, 20 October 2005; DIS ANON R2, Shrivenham, 28 October 2005.

[72] Presentation given by a senior DIS official to the OIG under Chatham House Rules, March 2007.

[73] *Ibid.*

[74] Arno Reuser presentation on open source exploitation to Netherlands Intelligence & Security Community, available at: http://www.oss.net

[75] Intelipedia is simply a US IC internal version of Wikipedia, utilising 'wiki' software to facilitate and perhaps enhance collaborative working. Wiki is Hawaiian for fast or quick. Of course, having such a 'sharing' system does not compel people to share. See: http://www.usnews.com/usnews/news/articles/061029/6outreach.htm; In a similar leveraging of the power of the Internet, in March 2005, the US IC, under the direction of the Foreign Military Studies Office, set up a web portal displaying thousands of Iraqi documents captured in 2003 requesting their translation by members of the public - 'Operation Iraqi Freedom Document Portal'. It was closed down in November 2006 after allegations that some of the documents contained information on how to prime a nuclear bomb, see: http://en.wikipedia.org/wiki/Operation_Iraqi_Freedom_documents and http://www.nytimes.com/2006/11/03/world/middleeast/03documents.html?ex=1320210000&en=b299ceb7b0f65500&ei=5088&partner=rssnyt&emc=rss but perhaps the real issue was exactly who does intelligence work in the US.

[76] Presentation given by a senior DIS official to the OIG under Chatham House Rules, March 2007.

[77] Interview, 2007 EUROPOL 5.2, by telephone, 4 January 2007.

[78] *Ibid.*

[79] The UK established the UK Intelligence Community's Open Source Joint Working Group (OSJWG) in 2000. It was publicly recognised for the first time in the Intelligence and Security Annual Report 2005-2006, 20 June 2006, report No: Cm 6864, p.8. The Professional Head of Intelligence Analysis (PHIA) also has

responsibility for the development of open source exploitation. The initial membership of the OSJWG was restricted to membership of the Single Intelligence Agency and DIS. Today the membership is more fluid, inclusive, and cross-sector. The group meets regularly up to ten times a year or so.

[80] In the US, the creation of the Open Source Center was approved by the DNI on 8 November 2005, see: https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html

[81] The BBC Monitoring Service is now known as simply BBC Monitoring. For a more comprehensive history of BBC Monitoring's establishment, see: Olive Renier, Vladimir Rubinstein, *Assigned to Listen: The Evesham Experience 1939-1943*, (London: BBC Books 1986), p.9-23.

[82] Intelligence and Security Committee, (Ed) 2006, *Annual Report 2005-2006*, Cm 6864, p.20.

[83] Green, A., 2006, 'More than just a building – The Story of GCHQ's New Accommodation Programme', presentation to Cranfield University at the UK Defence Academy, Shrivenham, 16 January 2006.

[84] This notion is supported both by a former senior intelligence professional and senior civil servant at separate meetings of the Oxford Intelligence Group held under Chatham House rules.

[85] Private correspondence with Director of UK Defence Academy's Conflict Studies Research Centre.

[86] This was the reason given to the author in 2005, by both GCHQ and HMRC, as to why no further engagement with the author through an in-depth case-study could be undertaken.

[87] Gibson, S.D., 2005, 'In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk', Globalisation and Changing Societal Expectation, *Risk Management: An International Journal*, 7, 4, pp.23-41.

[88] Accessed at: http://www.oss.net/extra/news/?module_instance=1&id=1334 dated 19 August 2005 on 25 August 2005.

[89] As far as the author could tell, the two papers were very similar if not identical.

[90] The Ethiopian/Eritrean hostage crisis of 1-16 March 2007 might prove to be an example, and it is unlikely that 'airwave' diplomacy as part of the policy response to the Iranian UK hostage crisis of March-April 2007 could have been managed without BBC Monitoring. Similarly, the open source effort at the UK's Primary Joint Headquarters was tasked in 2007 to examine the possibility of 'expeditionary' open source cells.

[91] 'Search smart' is how it was described to the author rather than a specific title.

[92] Interview, 2007, OSJWG 2, Cheltenham, 28 March 2007.

[93] Donald, D., (Ed) 2006, *After the Bubble: British Private Security Companies after Iraq*, Royal United Services Institute, Whitehall Paper 66; Friedman, G., 2004, *America's Secret War: Inside the Hidden Worldwide Struggle Between the United States and its Enemies*, London: Doubleday, Random House.

[94] In the special 'open source intelligence' issue of the US DOD's Military Intelligence Professional Bulletin (October-December 2005), available at: http://www.universityofmilitaryintelligence.us/mipb/issue.asp?issueID=6 , nowhere does it articulate how or why open source contributes.

[95] US Department of the Army, 2006, *Field manual Instruction 2-22.9: Open Source Intelligence*, dated 5 December 2006, available at: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf pp.A1-3.

[96] US Office of the Director of National Intelligence, 2006, *Intelligence Community Directive 301: National Open Source Enterprise*, dated: 11 July 2007, Washington, DC., available at: http://www.dni.gov/electronic_reading_room/ICD301.pdf

[97] Jeffson, J., 2005, 'Creating an Open Source Capability', *Military Intelligence Professional Bulletin*, 31, 4, pp.40-44.

[98] One of the reasons that ASD would monitor avian flu is because they have the language capability to translate reported outbreaks, which predominantly occur in Asia, its area of expertise.

[99] These IIRs have received 28 'major significance' evaluations from the DIA, NGIC, and NASIC alone. See the overall statistics on IIRs in the Appendices.

[100] Apparently OSC visitors to ASD in 2006 were surprised to see these and have subsequently subscribed to them themselves, which raises an interesting question with regard to duplication of effort, separation of organisational roles, the reality of virtual collaboration, and issues of scale for the likes of the US IC effort.

[101] Prosigns are equivalent to data fields of a database and have to be populated in a set and restricted way.

[102] See: US Office of the Director of National Intelligence, 2006, *Intelligence Community Directive 301, op cit.*

[103] Shown in interview with ASD 1 as being defined in: US Defense Intelligence Agency (DIA) Manual 58-12, *The DoD HUMINT Management System*, dated 30 June 1997.

[104] Comment made in discussion with ASD Interviewees 1 & 2.

[105] Contrary to popular belief, open source exploitation is formally conducted by all intelligence agencies within the UK Single Intelligence Account. The UK Open Source Joint Working Group (OSJWG) comprises SIS, SS, GCHQ, and latterly DIS and other agencies, precisely to exchange best practice and people.

[106] Private e-mail communication from these two agencies.

[107] See: US Office of the Director of National Intelligence, 2006, *Intelligence Community Directive 301, op cit.*

[108] *Ibid*.

[109] Both Hazard Management Solutions and Exclusive Analysis have been forced down this route. The ASD have designated quality control officers as the final stage of production.

[110] See: US Office of the Director of National Intelligence, 2006, *Intelligence Community Directive 301, op cit.*

[111] Herman, M., 2005, Getting Value out of Intelligence: A British Experience, *Intelligence Consumers Conference*, Stockholm, 29 August 2005,

[112] Press statement and briefing for the press at US DOD, 12 February 2002. The notion of 'unknown unknowns' has been a dilemma for risk management communities for some time. It is deployed in support of

argument from both the 'left' and the 'right'. It is interesting that that such a strong creature of the 'right' should use a phrase that Greenpeace, a creature of the 'left', regularly uses in support of their argument that the absence of evidence is not evidence of absence! See: Grove-White, R., 2001, New Wine, Old Bottles? Personal Reflections on the New Biotechnology Commissions, *The Political Quarterly Publishing Co. Ltd.*, 2001, 3, pp.466-72.

[113] Private conversation with Director of Intelligence Analysis at HMRC, May 2002.

[114] EUROPOL was attempting to establish some form of knowledge management structure in 2003; but the cultural resistance to the endeavour was readily apparent.

[115] OSS Conference November 2003 – Head of US DoD library staff.

[116] HMS is often asked whether it has secure facilities for classified information storage.

[117] Hulnick, A.S., 2004, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Westport, CT: Praeger; Berkowitz, B.D., Goodman, A.E., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press.

[118] Interview with Director HMS.

[119] FAS have reports on this – find.

[120] Kindsvater, L.C., 2003, The Need to Reorganize the Intelligence Community, *Studies in Intelligence: Journal of the American Intelligence Professional*, 47, 1, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol47no1/article03.html

[121] Hulnick, A.S., 2004, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Westport, CT: Praeger.

[122] See Interview with DIS Analyst Anon R1 in the Appendices.

[123] For 'sharing' as mandatory, see: US Intelligence Reform and Terrorism Prevention Act, 2004; US Presidential Executive Order, No: 133888, 2005, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, available at: http://www.fas.org/irp/offdocs/eo/eo-13388.htm ; US Attorney General, 2003, *Memorandum of Understanding Between Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing*, dated: 4 March 2003, available at: http://www.fas.org/sgp/othergov/mou-infoshare.pdf ; BG Thompson, *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*, (Washington: US House Committee on Homeland Security Democratic Staff 2006); RAND National Security Research Division & Office of DNI, *Towards a Theory of Intelligence*, (Washington: RAND 2006), p.1. For 'not sharing' doing damage, use: http://www.fas.org/blog/secrecy, and search using "sharing" . As one example see: http://www.fas.org/sgp/news/secrecy/2005/04/040805.html#2

[124] Conversation with a J2 representative from the UK Primary War Headquarters, 22 February 2007.

[125] For example, the notion of diversity was advocated by a leading UK open source practitioner in a presentation to the Oxford Pluscarden intelligence conference under Chatham House rules on 15 February 2007.

[126] Surowiecki, J., 2004, *The Wisdom of Crowds*, London: Little Brown; Rheingold, H., 2002, *Smart Mobs: The Next Social Revolution*, Cambridge, MA: Basic Books; Reynolds, G., 2006, *An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government and Other Goliaths*, Nashville, TE: Nelson Current; Levine, R., Locke, C., Searls, Doc., Weinberger, D., 2000, *The Cluetrain Manifesto: The End of Business as Usual*, Cambridge, MA: Perseus Books Group.

[127] See note 11 above and McMurray, J., 2006, 'Social Search Promises Better Intelligence', Associated Press, 9 July 2006, available at: http://msnbc.msn.com/id/13740161/

[128] In both the US and UK 'champions' of the analytical profession have been established.

[129] BBC Radio 4, 2007, *Falklands 25: A Dangerous Interface*, 2 April 2007. This was a special broadcast to mark the 25th anniversary of the Falklands War, in which Professor Alex Danchev (Professor of Political Science, Nottingham University) noted the similarities the two reports highlighted between the inattention paid to open source prior to Argentine invasion in 1982, and the débâcle of information concerning Iraqi WMD in 2003. Indeed, as Professor Richard Aldrich points out there is much in the post-Falklands War Franks Report that receives a similar airing in the post Iraqi WMD debacle reports, see: Aldrich, R.J., 2005, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, 16, 2005, pp.73-88.

CHAPTER FIVE

ANALYSIS AND DISCUSSION

(WHICH TRUTH, TO WHICH POWER, ABOUT WHAT, BY WHOM?)

> "A greater effort also should be made to harness the vast universe of information now available from open sources."
>
> Aspin-Brown Commission, 1996[1]

5.0 Introduction

The analysis and discussion of the research data - the findings - is in two parts. First, and principally, an analysis of the contribution of open source exploitation to intelligence based upon the empirical evidence of Chapter Four. Second, a discussion of the wider implications of open source exploitation for intelligence in the context of the relationship between intelligence and politics. The former might usefully be thought of as the operational consequences, the latter as the contextual significance. Both treat the simple question - 'so what?'

5.1 Part One: Operational Consequences

> "Compared with the more traditional or esoteric intelligence techniques, it [OSINT] is often faster, more economical, more prolific, or more authoritative."
>
> Herman L. Croom, 1969[2]

The literature review shows that there is nothing new in the exploitation of open sources of information for intelligence purposes. The literature also shows, by its paucity as much as anything, that very little effort has been expended in trying to understand exactly how open source exploitation contributes to the overall intelligence function, either absolutely or relatively to closed. Given the contemporary step change in ICT, which has brought open source exploitation to its present degree of prominence, it seems an appropriate time to

understand that contribution in order to further the discussion surrounding appropriate policy, doctrine and resource for an intelligence community's exploitation of open source information. The research methodology was designed to generate a model of this contribution by layering case-study upon case-study to discover how producers and users of open source understood what it was for. This section summarises the contemporary history of open source exploitation (technical, social and cultural), places the contemporary contribution of open source exploitation discovered in this study against that history, and discusses the implication for future policy.

5.1.1 Open source exploitation: its modern history

The formation of institutional 'state-sponsored' organisations by which open sources of information are exploited for 'modern' or 'industrial' intelligence purposes can usefully be pegged to the creation of the UK's BBC Monitoring Service in 1938.[3] Its US equivalent - Foreign Broadcast Monitoring Service, later Foreign Broadcast Information Service (FBIS) and now the Open Source Center (OSC) - emerged in 1941.[4]

Both were formed in response to the technological development of radio, in particular, its use in the 1930s as a tool by the Axis Powers, for the dissemination of propaganda. Interestingly in today's context, BBC Monitoring's first listening assignment was Arabic broadcast from Italian and German radio stations following the second Italo-Abyssinian War of 1934-37. This was followed by Spanish and Portuguese broadcast directed at Latin America.[5] Not only did they monitor broadcast media as a collection activity in its own right, but they also gauged the response to our own propaganda broadcast as part of a wider and more nuanced information operations campaign; much as they do now.

That 'monitoring' became categorised as 'open' and 'interception' as 'closed' or secret intelligence, was largely a reflection of the intended nature of the data transmitted - public versus secret. However as the two world wars merged into the Cold War, the predominance of secrecy became as much a reflection of the culture and imperatives of the

time as of the data collected and intelligence produced. Open source exploitation was a junior partner to the revealing of closed secrets; although, in the UK, organisations like the Soviet Studies Research Centre evolved alongside the BBC Monitoring Service to chip away at mysteries and intentions through examination of open source publications.

Thus, and unsurprisingly, secret technical intelligence collection, notably that derived from satellite platforms and Sigint activity, dominated the capabilities-oriented intelligence requirements of the Cold War. The closed nature of 'Eastern Bloc' society prompted an equal and opposite clandestine response from western powers.[6] The principles, values and ethics of this secret intelligence war were inevitably internalised and institutionalised as policy, doctrine and practice by the intelligence community of the time. Yet, the legacy of that time remains a substantial influence upon today's intelligence community, recognised by many of its own leadership as somewhat at odds with the present, so-called, information age. Today, in light of both the changing nature of contemporary society and the more recent changes in technology, RAND, equally unsurprisingly, has revisited the question of whether it is the product or the action of intelligence, which should be classified.[7]

The more recent scientific advance - digitisation - is merging with that significant cultural influence - globalisation. Indeed, some argue that the transformation in information and communication technology, associated with digitisation, is a root cause of the contemporary incarnation of globalisation.[8] It is also argued that globalisation and technology generally are influencing the evolution and development of so-called 'new risks' that intelligence and security organisations are increasingly directed to confront: WMD proliferation; pandemic disease; transnational crime; dual-use technology; critical national infrastructure vulnerability; emerging regional powers; resource competition; climate change; and demographic change amongst others.[9]

Information science now plays its part alongside all the other developed technologies that have hitherto been absorbed into the intelligence process and were simply not available to the intelligence community (let alone the public), when the Berlin Wall was rendered

redundant less than two decades ago. The exploitation of open source information - information legally available in the public domain - has ballooned commensurate with the transformation in ICT and the 'opening up' of formerly closed societies. Not only is the demarcation between open and closed intelligence seemingly more difficult to distinguish at an operational level today, but also the organising principle for the intelligence community - the security of the nation state - is more difficult to identify in terms of a unique threat, when set against a backdrop of emerging so-called 'new risk' sources.

Interestingly, and presaging the nature versus character distinction discussed below, even the establishment of the BBC Monitoring Service in 1938 was not an entirely new departure in the exploitation of open sources of information, or indeed its formalisation. In 1826, Henry Brougham, the radical Whig politician, established the Society for the Diffusion of Useful Knowledge in the UK. Its aim was: 'to impart useful information to all classes of the community'.[10] This aim sounds strikingly similar to that of Google's today: 'To organize the world's information and make it universally accessible and useful.'[11] Both implicitly profess utopian dreams of knowledge transforming society. Yet, one might enquire of both organisations - for what purpose. Contemporary open source evangelists like Steele also pioneer this utopian vision for the exploitation of open source information.[12] The Society wound up in 1848. Its product was considered too diverse, erratic, miscellaneous and non-controversial. One might add idealist and naïve; absent of purpose and ignorant of the long historical narrative of power oriented human engagement that is politics. It had confused nature with character; purpose with conduct. It thought that the provision of information was the end game and in doing so elevated means to ends.

Today all security, law enforcement, and defence establishments undertake open source exploitation for intelligence purposes. Some openly and formally declare it. Others do not. Some establish deliberate and discrete exploitation efforts, others leave it to analysts. Furthermore, it is exploited across all sectors of society and collaboration between sectors

is commonplace. Regardless, the exploitation of open sources of information offers certain benefits peculiar to it.

5.1.2 Open source exploitation: Nearly new, but not quite

> "Given the operational tempo and the environment, classification is not a good thing but a necessary evil. This is even more evident in sharing information with coalition partners."
>
> Eliot A. Jardines (Assistant Deputy DNI Open Source), 2006[13]

Today, the volume of information is expanding. Its availability is increasing. Its exploitation is itself subject to other technological developments. The transformation in information and communication technology (ICT), notably digitisation, mobile connectivity, data management, and the Internet, now present additional platforms by which to exploit information for intelligence purposes. It is almost an holistic all-source capability in its own right: satellite imagery is available commercially off the shelf to anyone with a credit card; 'news' can be aggregated, searched and sorted by anyone with a telephone connection and an Internet Service Provider; the 'citizen journalist' or 'blogger', alongside the CNN effect, is increasingly first to reveal the mystery of 'uncertainty' in real time; and 'mashing-up' on a 'semantic web' or the sharing of intelligence via an 'intelipedia' moves analysis towards a real-time product.[14]

Intelligence communities know this. Indeed, the growing significance of open source exploitation today is simply an evolution of what has long been undertaken. Its nature and purpose have not changed. Its character is merely adjusting and updating for the contemporary context, commensurate with evolving technological and socio-cultural influences.[15] It is the institutionalised organisational and cultural barriers of bureaucracies that have to adjust to what is intuitively recognised by individuals within those institutions.

Equally, the culture of secrecy, which characterised approximately 50 years of state-run intelligence gathering during the Cold War, if not being hammered by these external

'competitors', is proving more difficult to sustain in a global knowledge-driven society, where sharing is increasingly regarded as more critical than not sharing.[16] Indeed, as some of the case-studies have argued, the distinction between open and closed is becoming more difficult for intelligence agencies to resolve.[17] This is not to say that the security of sources, methods and intentions is suddenly rendered invalid. Operational security is a long way from the culture of secrecy; but the two should be differentiated honestly.

In fact, mature intelligence agencies are deliberately finding new ways to integrate open and closed information sources. They recognise that what does not change in the nature of the information business is the enduring and crucial significance of analysis; the importance of making sense of the information that is collected.[18] In this regard, it is irrelevant whether the information is open or closed, rather that fundamental characteristics such as validity, utility, reliability, and bias are established, and that it contributes to wise judgement in the face of uncertainty in a timely manner. To paraphrase Keegan - who knows what, in sufficient time, to make use of it.[19]

The total information business and the effectiveness of intelligence seem linked. In 1969, Croom summarised much of the contemporary debate, the potential benefits, and the key policy issue of resource allocation surrounding open source exploitation in just seven well-crafted pages. He argued a case for the 'efficacy' of open source exploitation using nuclear weapons proliferation together with the developing international situations of Africa, Latin America, and South East Asia as examples! He further suggested the establishment of an open source agency - outside the dominant (at the time) CIA - specifically instructed to treat the then new intelligence species.[20] If the dates were changed, one might be forgiven for thinking that Croom's paper was contemporary. If a novice to the debate about open source were to read nothing else, it would sufficiently circumscribe the argument.

What does seem new in the intelligence discipline is the formal and deliberate exploitation of open sources of information within the traditionally closed agencies of the intelligence

community. That is to say that over the last ten years or so, with one or two exceptions, open source intelligence 'cells' have been formally established and resourced within security, law enforcement, and defence organisations specifically to deal with increasing open source data. Some agencies are rapidly absorbing and embracing it, others less so; but it is happening. Arguably, the classical role of intelligence - secret state activity designed to understand or influence foreign entities - now reflects another time.[21] Warner's 'minority' definition in 2005: 'Information for decision makers' more accurately reflects the diminution in distinction between open and closed information today.[22] Similarly, the sequential model of the intelligence cycle seems increasingly difficult to sustain in the networked world and may now only have relevance to the individual practitioner rather than any process or system.[23] Thus, while Johnson's call for a theory of intelligence seems entirely apposite,[24] the notion of a theory of intelligence seems intractable, while its definition reflects its character or conduct rather than its nature or purpose.[25]

Open source exploitation is not the be-all and end-all of intelligence. The oft-quoted estimate that 80 percent or more of final intelligence product is generated from open source exploitation is a mischievous 'red herring', regurgitated anecdotally since Allen Dulles stated it in 1947.[26] Moreover, a broad estimate of the contribution of open source simply does not equate to all intelligence targets equally, or at the same time.[27] In the mid 1990s the US government's (CIA) Community Open Source Programme had officially estimated the overall open source contribution to be in the range of 40 percent, while specific contributions depended upon target difficulty. Thus it might range from ten percent in very denied-area secret-issue matters, to 90 percent on international economics.[28] Anecdotal evidence is one thing, but the danger of apocryphal evidence for the sake of allocating a number is a trap worth avoiding.[29] The obsession should be with the meaning behind the number rather than the number itself.

Nor, for that matter, is it terribly significant that closed sources constitute the remaining 20 percent. Percentages might usefully represent arguments about the efficient allocation of

resources - an important discussion - but they do not reflect testimony to effectiveness. How do you know that open source constitutes 80 percent? What is the yardstick of measurement? And anyway - so what? Surely, it is effectiveness that matters? Of course, as Odom, the recent RAND conference, and Gill and Phythian have noted, intelligence effectiveness is an extremely slippery concept to pin down, let alone measure.[30]

Yet, effectiveness as an expression of meaningful outcome seems more relevant than efficiency expressed as a relationship between inputs and outputs. In this regard, ethnographic studies of what actually happens together with historical case-studies seem more likely to produce rich and meaningful narrative as interpretation of outcome than statistics. Furthermore, outcomes should relate ontologically to the ideological purpose of contemporary society rather than to customer-focusing quantitative metrics of self-satisfaction, surprise-free zones, or enhanced decision-making. These are pseudo-scientific initiatives designed to satisfy the 'process-junkies' of contemporary managerialism rather than signatures of the fundamental contribution of the intelligence function. Until it becomes evident as to what societies stand for, intelligence including the exploitation of open source will meander, like other institutions, satisfying risk management as process and ends in its own right rather than purposeful objectives.

One of the main reasons that open source is valued, as the research found, is because it can be shared; not so that transparency and accountability procedures can be 'ticked-off', but to propel power, through access to a deeper and broader knowledge base, towards a better understanding of reality than it might otherwise have.[31] In an evolving epoch characterised by the ubiquity of information, the old adage that intelligence's role is to tell truth to power remains. It is just that power is spreading beyond government and state towards a societal commons, while 'truth' is required on an increasing variety of risk.[32]

Here lies another virtue of open source discovered in the research - whether harvested by the intelligence community or not - as resource for independent and diverse analysis, in order to more accurately evaluate risk. Both policy-maker and knowledge-worker are

responsible for ensuring that the collectively formed representation of reality is as accurate as possible, and the purpose for which it is formed is clear. That will necessitate establishing what we are for and that will only be achieved, like it ever was, by politics. More preferable that it is harvested by the intelligence community on behalf of society as trusted providers of truth to an expanded power, than from elsewhere - not an easy journey to undertake.

5.1.3 The high order factors model

Sharing and analysis were not the only factors discovered. The research across contemporary intelligence and law enforcement organisations established seven high order factors describing the contribution of open source exploitation - its effectiveness - to the wider intelligence function:

- **Context.** Without exception the case-studies all recognise that open sources of information represent a 'matrix', in which to conduct the entirety of their work. Described variously as: 'a first port of call'; 'stocking filler'; 'background'; the 'can-opener'; or 'landscape', it represents the most widely acclaimed attribute of open source exploitation. Rolington's description of President Clinton's frustration with the intelligence of the 'Presidents' Daily Brief' summarises the significance of context.[33]

- **Utility.** Utility was often mentioned as synonym for speed, volume, and cost. Practitioners consider it quicker, more productive and cheaper to exploit open sources of information than closed. Thus, it is more immediately useful to analysts. However, utility is also understood to connote a notion of 'value-added' - a sense that the information derived from open source exploitation actually creates value for the customer; that it possesses useful benefit in its own right and is worth paying for. Both public sector analysts and commercial private information brokers alike report this attribute. Arguably, the element of usability precedes and stimulates the notion of

communicability - the sharing of information. Thus, this aspect of 'usefulness' seems to straddle both utility and communicability.

- **Cross-check.** The emphasis on this factor comes from the now extensive use of open source information within traditionally closed single-source intelligence collection agencies. These agencies clearly recognise that it is simply uneconomical and unprofessional to disseminate intelligence product derived from closed sources when it already resides in the open domain. Furthermore, this notion of cross-checking as benchmark is used two-ways, in the sense that closed information can also be used to disprove, dispute, or challenge open source information.

- **Focus.** Focus connotes direction as well as acuity. Direction suggests the targeting onto another subject as a result of research - an alternative 'lead'. Acuity suggests the depth to which a subject is examined or the granularity which is revealed by research. Thus, focus here has two meanings for open source exploitation - depth and direction. Additionally, the focusing of closed sources by open ones arguably reduces the amount or degree of downside risk that closed methods take on, whether physical or ethical.

- **Surge.** Clandestine intelligence, particularly 'Humint', is not an activity that can be turned on and off like a tap. Conversely open source information, which is already 'out there', distributed, and reflecting an amalgam of all intelligence disciplines is more easily manoeuvrable to new targets and requirements than the traditional collection sources. In this regard open source exploitation offers a significant surge capability in demanding times until closed means can be brought to bear as appropriate.

- **Communicability.** One of the constantly repeating themes of the intelligence enquiries of 2004 was the inability of intelligence agencies to share information with each other, and governments to communicate risk to their publics. It is not only nation-state intelligence communities that recognise this. International organisations including the EU, NATO, and UN have recognised the need for information

cooperation and exchange, particularly in the arena of counter-terrorism.[34] The notion of security is often cited as rationale for an inability to share, whereas issues of bureaucracy, technology, culture, and politics are equally complicit. Indeed the Federation of American Scientists has uncovered several reports that point to increasing *in*security as a result of not sharing.[35] Theoretically, it should be easier to share information that is derived from open sources given that it is legally available in the public domain. Additionally, it becomes possible to release or disseminate the product of otherwise closed sources once available in the open domain. The security aspect then shrinks to who collects it rather than who from. Whether open source will punch through the cultural, institutional and political barriers to sharing remains to be seen.

- **Analysis.** Analysis broadly comprises five varieties, each of which is variously undertaken by open source organisations:
  - Current intelligence in order to maintain information on developments of current crises, events and situations.
  - Database or knowledge creation in order to surge capacity for future events.
  - Forecasts that estimate future developments.
  - Warnings and indicators in order to alert that a crisis is looming or begun.
  - 'Red Teaming' or 'devil's advocacy' in order to question existing analysis, its assumptions and conclusions based upon alternative information sets and/or alternative analysts. The value of open source 'red teaming' is that it can be conducted both within the intelligence community or contracted from outside it, thus dealing with both of Betts' advocacy questions - multiple internal and 'devil' external - in one go.[36]

The degree to which the collectors of open source undertake analysis varies considerably. Undoubtedly, information is filtered, processed and framed as it is collected. Open source information is no less demanding of the witting or unwitting virtues required of objective assessment than closed. However, in private information brokerages, both collection and analysis tend to be undertaken by the same individuals,

or groups of individuals comfortably interchanging between all elements of the intelligence cycle in order to create product. In public sector agencies, analysis seems entrenched with those designated as analysts. Here, open source procedures vary between either 'push' or 'pull' systems. In some agencies a 'push' system operates whereby open source expertise sits (literally) alongside an analyst or team of analysts. In others a 'pull' system operates where analysts have to go to centralised open source cells with requirements and wait for a response.

The potential to 'red-team', 'counter-analyse' or present alternative analysis is particularly pertinent. In the absence of an alternative data set only the analysts can be varied. With open source, both data and the analysts can be varied; the latter from outside the intelligence community, thus correcting the criticism of a tendency toward the oft-quoted heuristic of groupthink. This presentation of a separate data set and analysis alongside that derived from closed sources has both operational and strategic benefit. At an operational level, alternative interpretation of security risks emerge. At a strategic level, the essential validity of those risks can be audited from the outset.

Three other potential high order factors were discounted: serendipity; horizon-scanning; and diversity. Serendipity is not an unfamiliar ploy within the intelligence community. This author's own intelligence experience gave him licence to pursue 'interesting' avenues outside given requirements. Such a capability is regrettably seen as wasteful in today's just-in-time, lean supply chain, target-driven economy; it is a brave institution that will sanction 'research' for research's sake, absent of measurement, and be seen as counter-cultural. Yet, in the world of risk management, the notion of making one's own luck, recognising it when it happens, and exploiting it if it does, is a refreshingly new topic for the risk management discipline.[37] Similarly, there is growing recognition in the risk management world that the equal and opposite notion of 'misfortune' can militate against one with the same unpredictability.[38] Both are characterised by uncertainty in the true dictionary definition of the word. The importance of horizon scanning appears in many contemporary UK security programmes, but with little attendant capacity to deliver it.

Furthermore, the analogy of horizon scanning seems rather weak if security threats are lined up just over the horizon. It might be better to have sensors beyond the horizon rather than scanning it. The important point here is that just as serendipity is not exclusively an open source happenstance, horizon-scanning is not a uniquely open source prerogative. Other intelligence disciplines are as likely to experience serendipity as they can be directed to perform horizon-scanning duties. They are rejected as not being significantly exclusive to open source exploitation. Furthermore, they are simply not universally reflected in the research data. Diversity, on the other hand, is clearly something open source exploitation projects might claim to offer that other intelligence collection disciplines cannot. Indeed, the process of analysis and assessment cannot truly claim to be comprehensive if it is not seen to comprise an all-source input. The fate of diversity as a contender for the high order factors model has been difficult to determine. It is discounted for four reasons. First, it is simply too broad a descriptor. As Chapter Four suggested it can be applied to each of the high order factors. Second, it is the duty of all intelligence conduct to consider the range of possible forecasts before either agreeing to disagree or collegiately coming to a single view. Third, it was barely mentioned in the research beyond dialogue with one very senior open source practitioner. Fourth, in the present context, diversity has so many connotations stretching far beyond the practice and study of intelligence that it might be a confusing factor to include. On balance it is rejected, but it does seem a worthy objective, in the strict sense of intelligence in support to decision-making.

The exploitation of open source information in the UK public sector is evolving piecemeal. Overarching policy, doctrine, and training have been absent until hitherto. However, the recent creation of an 'open source champion' and a Joint Working Group directing efforts towards such policy, doctrine and training is addressing that.[39] In the US, the creation of the DNI Open Source Centre out of FBIS in November 2005, at least reflects commitment to open source exploitation at the highest level.[40] These respective approaches - UK procedural versus US structural - reflect the different culture, traditions and resource of both intelligence communities rather than any inherent effectiveness of OSINT. Additionally, the private sector has its own way of exploiting open sources, as do other

national intelligence communities that do not possess the closed resources of the UK or US. Yet, all approaches to exploiting open source are almost immaterial if they are to be judged by their conduct rather than their efficacy. It is the outcomes and contribution of open source exploitation to the nature and purpose of intelligence that are more significant.

Thus, the challenges for the total information business, of which OSINT is a part, are not simply how to deal with the increasing volume of information, or the sharing of classified sources. These can be dealt with procedurally by technological means and culturally by attitudinal shifts. The greater challenges are:

- How to deal with the spread of information and knowledge as the ICT transformation shifts and their availability throws up competing representations of reality influencing the balance of power within and between societies let alone intelligence communities.
- Whether the balance between open and closed resources and capabilities are reflected within intelligence communities.
- How to reconnect society with a sense of purpose in the sense of what we are for, rather than deferring to process or a sense of what we are against.
- How to regain a sense of confidence in knowing, rather than measuring, that what intelligence does is effective.

'Route 101' of salesmanship is to sell the sizzle in the sausage before the sausage. That is to say sell the value or benefits of something before its features or solution. These high order factors can be taken to represent the sizzle to immediate customers but the sausage remains meaningful outcome.

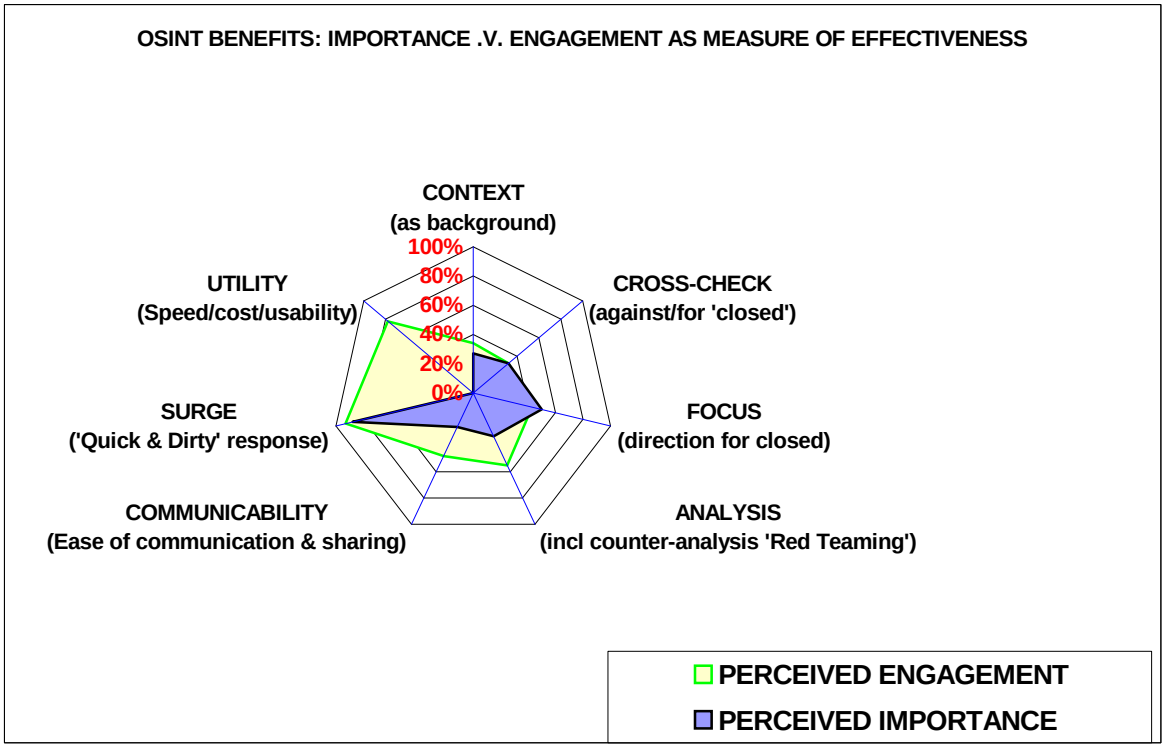
5.1.4 What to do with the claimed 'benefits'?

> "The Government Performance and Results Act (GPRA) requires agencies to set goals and objectives for their performance, and to measure progress against these goals and objectives."
>
> Raphael Perl, 2005[41]

Perl's report, from which the above quote is taken, goes on to acknowledge that measuring the effectiveness of the 'global war on terror' is not easy: "(T)here is currently no common set of criteria for measuring success."[42] There are no readily available variables. Progress is assumed to be a positive entity. What can be measured - incidents, deaths, arrests - become the *de-facto* demonstrators of success. What cannot be measured - intention, perception, reaction - are recognised as problematic. The report concludes with three potential 'measurements': 'incidents' - the number of attacks; 'attitudes' - represented by behaviour, confidence, polarisation, sentiment and bigotry; and trends - changes in the above two; but no sense of how one begins to incorporate them into a meaningful measurement or model. This may be because such a measurement is mechanistic and fails to capture any ontological aspect.

If measurement is necessary, then perhaps two useful, but inherently subjective, 'measures' need to be imposed upon this research's model, beyond the seven factors identified, which treat the high order factors as not simply descriptors of contribution but objectives in their own right. It is tentatively suggested that these measures might be 'perceived importance' and 'perceived engagement'. Figure 5.1 below serves as illustration. A measure of importance might best be undertaken through surveying OSINT's customers for their interpretation of the value-added by open source product, much as many open source cells now do. A measure of engagement might be derived from a more holistic examination of the OSINT process itself, either through self-examination or by external oversight, in order to determine appropriate resourcing, financing, and direction for open source exploitation. Combining the benefits identified in the model with measuring them as objectives in their own right begins to incorporate notions of effectiveness and efficacy rather than merely efficiency. However, some assumptions, consequences, and limits arise beyond the scope of this research to challenge: that turning the factors into objectives internalises them to the intelligence community rather than becoming anything externally meaningful to society; that these extra measures are valid; or that the inevitable relative comparison between closed and open sources is welcome to begin with.

Figure 5.1: High order benefits as objectives for open source exploitation effectiveness



Source: Author

Effectiveness and efficacy should not be confused with efficiency: efficiency is a measure of how inputs to a process are 'turned' into outputs with minimal waste; effectiveness is the extent to which a measurable output is obtained as a result of the process; and efficacy is a measure of that outcome against desirable objectives - how the outputs of the process relate to objectives set for it.[43] Efficiency and effectiveness, although extremely important, seem best divined internally to an organisation, and perhaps the measures of importance and engagement with regard to the high order factors described above might find traction there. However, efficacy - the achievement of objectives set - seems the more critical yet illusory prize of most organisations and processes.

Objectives may end up as targets and service level agreements, rather than meaningful outcomes. Contemporary discussion surrounding the setting of targets suggests that target setting and service level agreements only end up being measure of efficiency and effectiveness rather than efficacy. In 2005, the UK education system of examination was

likened to 'taking penalties' without understanding the game of football. The UK Intelligence Agencies (within the SIA) are audited by the National Audit Office. They: "are subject to close budgetary scrutiny and challenging efficiency targets".[44] Furthermore, the expenditure and resource allocation of the Agencies are subject to Parliamentary scrutiny through the Intelligence and Security Committee. Nowhere, is effectiveness mentioned, and the measurement that does exist is not community-wide, which makes the value-added of open source effectiveness difficult to display when it is so clearly exploited throughout the entire community.

The challenge for all public sector organisations, absent the bottom line of commercial organisations, is setting meaningful outcomes as objectives. This is particularly the case for the intelligence community and no less so for the exploitation of open sources, with the singularly useful exception that OSINT has 'customers', who may not be able to measure the benefit of the received product in discrete quantitative terms, but will certainly have a qualitative view. In the case of OSINT, this chapter posits that the high order factors are the objectives, and meeting them is determined by the perceived 'match' between importance and engagement. A model that seeks to identify the effectiveness of its open source exploitation effort needs to 'measure' itself against meaningful outcomes, which in this case, and recognising the limits of internalisation and comparison, are the high order factors themselves. Again, this might best be achieved by an examination of the OSINT process through the eyes of its customers for importance and by the organisation's directors and auditors for engagement.

5.1.5 Open source policy and doctrine

> "Which search engine would you recommend?"
>
> UK Intelligence Analyst, 2007[45]

There is no nationally coordinated, nationally pursued open source exploitation policy or doctrine within the US or UK intelligence communities.[46] However, there is effort in both communities to correct this. The US has created a National Open Source Enterprise to

begin such an endeavour on top of the 'central' Open Source Center within the DNI headquartered at the CIA. Both communities have established open source champions. Additionally, the UK has established an open source joint working group (OSJWG) to pursue common best practice. It may also be pertinent to suggest that, in the UK at least, the OSJWG should pursue a deliberate professional project. A profession has as its constituents the following essential objectives:[47]

- A specific set of standards and code of ethics
- A body of knowledge - possibly embodied in a journal - beginning to create an historical perspective
- A recognised forum for discussion
- An authoritative body that can certify member competencies
- An educational discipline to prepare students and practitioners in the functions and philosophies of the profession

In the meantime, and based upon the broad research effort of this thesis, the following points recommend themselves as considerations for a national open source policy or an organisational open source effort:

Resource

- The creation of a central (national) open source centre of excellence to coordinate policy and doctrine, establish practitioner standards, undertake training, determine ethical behaviour and construct a body of practitioner knowledge. The US embarked upon this in November 2005 with its Open Source Center incorporating FBIS along the way. It most closely resembles a centre of excellence although not an independent agency. For the UK, the combination of BBC Monitoring, the 'guild of expertise' in the OSJWG, and a host of representatives from such disparate open source users as Cabinet Office Assessments Staff through the UK Defence Academy's Conflict Studies Research Centre to the Metropolitan Police Service, Serious Organised Crime Agency and Joint Terrorism Analysis Centre would be an obvious parallel.

- Any open source effort requires a viable critical mass at its outset in order to develop intellectual practice internally and demonstrate practical contribution externally. It needs to be given a chance to succeed rather than no option but to fail. Equally, it does not want to expand so fast that it stretches too thin
- Successful open source exploitation necessitates expertise on several fronts beyond collection and analytical skill. These include commercial skills, the monitoring and incorporation of ICT developments, knowledge working, and source research. All of which needs to be permanently established and undertaken simultaneously and continuously.

Guidelines

The public sector open source community have developed a series of guidelines that best coin how they are trying to proceed:

- 'Collect once for the community' is the principle motto of the public sector open source community at least. Of course it runs counter to the motto of its commercial suppliers: 'build it once and sell it many times'. However, the acquisition of database or information resource on a community-wide basis is simply cheaper and more efficient for the taxpayer than the more prevalent fragmented and isolated nature of open source centres. This in turn will need an open source distribution network that links all the open source practices. The US has developed the Open Source Intelligence System (OSIS), and the '*opensource.gov*' World Wide Web presence, which address that issue. Indeed, the web presence is available to the UK intelligence community; a limited version has been made available to the author by virtue of being resident at the UK Defence Academy.[48]
- 'Incorporate expertise into the community' is another motto of public sector open source exploitation. By extension from the point above, it makes sense to incorporate expert analysis that traditionally lies outside the intelligence community. This is nothing new, but it is doubtful that formal record of expert witness on a global basis has been undertaken hitherto. This is more usefully interpreted as 'know who knows'

reflecting the fact that subject matter expertise inevitably and increasingly resides outside the intelligence community.

- 'Check closed against open'. Apart from avoiding reputational embarrassment, it provides a cross-check for open against closed, which is a cultural necessity in a climate where classified information is automatically prized above non-classified and therefore essential to proving relative effectiveness. This of course works both ways in the sense that something provided by closed means may not be available openly and thus proves effectiveness the other way (to a customer at least). It also facilitates sending the 'message' of a closed source via open means.
- 'Acquire not collect'. Given the vast volume of information available to open source collection and the tempo of contemporary decision-making, it makes sense to inculcate an attitudinal shift to collection that favours answering a question over collecting in case a question arises - just in time rather than just in case. It is one attitudinal response to the challenge of information overload alongside the deeply philosophical, but sensible, admonition: 'never let perfection be the enemy of good enough'.
- 'In the ring not in the dressing room'. Open source exploitation should be available at the point of analysis and production, either in the form of a specialist, or on the screen in front of the analyst. The effort required by the user or customer to obtain open source product and open source expertise should be minimised. Furthermore, open source expertise should be placed alongside the customer because customers want tailored product rather than centralised uniform product. It seems to be a developing misunderstanding that giving an analyst access to the Internet can somehow substitute for open source expertise across search techniques, language, data manipulation, information sources or time.

5.1.6 Exploitation models

The case-studies displayed as many methods of organising, as there were case-studies. However, two broadly distinct courses of action emerge, which have little to do with open source exploitation and much more to do with the culture of the open source team coupled

with the degree of 'buy-in' from the parent organisation. Open source expertise and product is either pushed to the user by the open source function or extracted from the open source function by the user. Pushing product to the user is characterised by placing open source specialists at the users elbow and streaming information to the user desktop. BBC Monitoring exemplifies this approach. Pulling information generally translates in reality into the analyst going to the open source cell.

The 'push' method creates two obvious advantages when specialists are placed at the point of analysis. First, it deliberately creates, or otherwise leaves, a 'centre of excellence' or 'backstop' for the more challenging open source requirements generated by analysts. Second, and probably as important, it creates a channel of communication between the open source specialist and the subject matter expert. These two combined begin to create the matrix that the preliminary model alluded to. 'Mixing with' the users also seems important at the outset of an open source effort, when its benefit can be 'sold' more effectively. This in turn requires 'buy-in' to create a sufficient centre of gravity in the first place.

It was outside the scope of this research to determine which method is more successful, preferable, or how one might determine such success. DIS and EUROPOL demonstrated the pull method most efficiently. Yet, both have had 'traction' problems within their parent organisations: EUROPOL's effort being disbanded in 2006, and the DIS effort reorganised in 2006. Arguably, the culture and sense of effectiveness that the open source cell established for itself generated a compliant and efficient pull model. Interestingly, the sheer layout of EUROPOL and the collaborative working relationships between departments and individuals supported this arrangement. However, the collaborative and compliant culture was not sustained. The DIS open source effort post-reorganisation remains unclear to the author.

Finally, in this section, and again not the focal point of the research, yet often raised in case-study interviews, is the notion that open source exploitation might be better conducted

from a single agency residing separately outside the other agencies. To a degree this already happens in the UK if one considers the semi-independent status of BBC Monitoring. But it remains 'semi' because its funding is controlled by its government department sponsors and its 'politics' tied to the BBC-government relationship as a whole. Similarly, the 2005-established OSC within the US DNI is presented as independent, although its budget and location, and thus its autonomy, reside firmly within the CIA. The arguments in favour of an independent open source agency are really an extension of the push model above. It would create a centre of excellence and concentration of resources at a national level, currently perceived best practice by some at an organisational level, which might deliver all the high order contributory factors that are pertinent to open source exploitation. Additionally, it would be a legitimate focal point for optimising standards, policy, training and doctrine across the intelligence community for open source. It removes an essentially minimally-classified operation from an essentially secret one and it removes a nascent intelligence source from culturally difficult and rigid traditional ones.

The counter-arguments include: the provision of additional resource in a notoriously tight public sector environment; the re-balancing of existing resource within the same overall budget; the increased inter-agency political 'turf wars' arising out of such a creation or new funding arrangements; the retention of considerable 'tentacles' within all the other agencies that may have greater political ramifications than existing liaison arrangements between agencies; and the not insignificant hypothesis that internal open source efforts may be more effectively conducted within agencies, particularly agencies that are culturally favourable and supportive. It begs the question again of how to determine efficacy.

The analysis factor is also substantive. Given the capability of open source exploitation to conduct similar, if not additional, collection techniques to closed collection, a separate open source agency might usefully be deployed to contribute an alternate all-source open source analysis for strategic decision-making, perhaps in the form of open national intelligence estimates for a national security or risk council, beyond the traditionally closed analysis. This point is explored more fully within the discussion of context below.

5.1.7 Open source cell structure

Throughout the course of the research study it became clear that alongside key contributing factors, the exploitation of open source necessitated some common vital expertise and skills. Mature open source cells include the following key functions:

- Research and subject matter expertise including links to external subject matter experts and databases.
- Language expertise for key targets including links to external translation services
- ICT research and development including links to private sector, academic, and government research establishments
- Information collection and on-line search specialists
- Publication, presentation, production, editing and media requirements for dissemination
- Commercial business and contract management
- Intelligence direction responsible for all aspects of the intelligence cycle
- Knowledge working expertise

They are not necessarily equally represented or always present, but they are universally recognised and desired (see Figure 4.6).

5.1.8 Challenges and barriers

The challenge of balancing resource

> "Hostile armies may face each other for years, striving for the victory which is decided in a single day. This being so, to remain in ignorance of the enemy's condition simply because one grudges the outlay of a hundred ounces of silver in honors (sic) and emoluments, is the height of inhumanity."
>
> Sun Tzu, 400-320BC[49]

Sun Tzu's *Sunzi Bingfa* had something to say about the amount of resource devoted to intelligence. The quote above implies that being too cheap to pay spies is both a false economy and socially destructive: "Such a man is no general; no support to his sovereign; no master of victory". (13:3)[50] He was referring specifically to the employment of spies; that was the sum of the intelligence world then. The Internet was not available to Master Sun. The notions of satellite imagery let alone open sources of information were not of his world. However, by comparison to today, his outlay for open sources would be considerably less than a hundred ounces of silver for spies. Doubtless his pragmatic approach to warfare would have relished their exploitation in pursuit of a greater purpose. Nevertheless, the general point about resource balance remains as vital today, notwithstanding the fact that choices are more nuanced. It is not merely a choice between to have or not have intelligence assets; rather what their precise composition should be. The nature, logic, and purpose of intelligence are not at issue. However, its character and grammar are entirely questionable in light of its changing context.

The US intelligence budget is estimated at approximately US$44 Bn, equivalent to roughly ten percent of its defense budget.[51] The UK budget is approximately US$3.2 Bn (£1.6 Bn) for the three principal Agencies constituting the Single Intelligence Account including capital expenditure.[52] These represent no small outlay and certainly no 'grudge'. Both intelligence communities have seen hikes in resource allocation since 9/11, beyond their Cold War capacity and funding in real terms. Yet, if 80 percent of its product and possibly a significant proportion of its efficacy reside in the exploitation of open source then one might reasonably ask the question - how much more efficient, if not effective, might it be with similarly proportioned resource?

Perceived barriers

The research indicates that several commonly held perceptions pertain to open source exploitation. They obtain almost as a counter-culture to the main findings of this research. The following are common:

- It is often opined that open sources cannot provide a sufficient level of granularity against a target that will create a 'smoking gun', concrete evidence, or 'point intelligence' - the when, where and how of events - that the traditional intelligence function aims to provide. The implication is that closed intelligence can. However, this either wilfully maligns open at the expense of closed or reveals a misunderstanding of the broad capabilities of intelligence in the round. Both the research enquiries with Hazard Management Solutions regarding global IED events and with PRA into single-issue activism indicate that open source is certainly capable of establishing trends and occasionally capable of forecasting target events. There is no mystery to this. In the first case, the simple fact is that when bombs 'go off' (and often when they do not, which of course provides even better forensic evidence) they are comprehensively reported. In the latter case-study, the medium of single-issue activism is the very same medium of open source exploitation: from the Internet and World Wide Web to pamphlets and posters. The key to success in both cases is not the collection but the capability and expertise of the analytical team interpreting the information.
- Again it is often heard said in intelligence circles that open source intelligence 'equals' the Internet and therefore 90 percent of it is unverifiable, untrustworthy, or simply 'rubbish'. This is not an unfair comment however difficult to establish in its own right. The counter-argument that open source practitioners deploy is that 90 percent of everything is 'rubbish', including closed information. Indeed, if Steele is correct, 90 percent or more of information collected covertly is not even analysed and so therefore by definition is rejected as genuine rubbish. The immutable law of anyone diligently engaged in the information business is to ascertain as best possible what is fact from fiction regardless of its origin.
- The most pernicious view is the notion that because open source is not covertly collected, and by implication its product not classified 'secret', it must by implication be inferior. Allied to this is a subordinate notion that information derived from the private sector is similarly inferior to that collected by the public sector. This is probably best captured and summarised by the testimony of Eliot Jardines (AD/DNI-OS) responsible for the US national open source effort and, therefore, while he holds

> the post, probably the most powerful global open source practitioner. He has publicly stated that he knows he is challenged to change a deep-rooted culture that says classification is the *imprimatur* for the validity of intelligence; but that, the intelligence community can no longer afford the mindset of the higher the classification, the more valid the information.[53]

These perceptions emerged from the research almost as background to the focal objective of understanding how open source genuinely contributes. Never very far away from the day-to-day activity of open source exploitation, expressed by many individuals interviewed in most of the organisations examined, is the sense of a cultural proclivity that is hostile to open source exploitation. Only where open source has achieved 'buy-in' from the board, or simply dominates the intelligence function such as in the private sector, are these perceptions challenged or absent respectively. Implicit in these perceptions is an underlying sense that closed information is simply by definition 'superior' to open. Yet, this cultural reaction is by no means universally expressed by all individuals within the community, or indeed by analysts specifically. Both DIS analysts interviewed suggested that open source was their 'banker' against a lack of closed, a delay in the arrival of closed, an inability to use closed, and the extraordinarily tight deadlines imposed upon their product in the first place that closed could not always meet.

It is outside the remit of this research to explore why this 'culturally-anti' yet 'individually-pro' position has emerged. Indeed, it may not even be a correct perception given that it was not deliberately being looked for. However, it would be interesting to test as hypothesis the hunch that has emerged in this research, and is reflected strongly in the literature, that the 'culture of anti' has been institutionally constructed by the established (possibly older) sections of the intelligence community. Alternatively, and perhaps more useful, it might be interesting to test a hypothesis that suggests the culture of 'pro' will rise, as a younger more techno-friendly generation of analysts occupy the establishment. The impression created throughout the research was that that they do not cast open source exploitation in such stark competition with closed as much as 'older' analysts. That the

whole open versus closed argument might simply transpire to be some generational aberration, reflecting the moral panic that saw the popular novel under pressure in the early 18th century in much the same way as the video game is perceived the scourge of today's younger generation, is an important sociological line of enquiry.[54]

Real barriers

Whether these perceptions are instrumental in obstructing the exploitation of open sources is outside the purview of the focal research aim. However, they are certainly present. In a similar vein real objectively understood barriers to open source exploitation also emerged as background to the main effort. They are also challenges for policy and doctrine. Principally, they include:

- **Language challenges**. Open sources of information are simply not delivered exclusively in English, as they are also simply not exclusively found on the Internet. The variety of languages required to fully exploit open sources is ideally the number of languages that are spoken. Resource constraints let alone the requisite skill base militate against this. At the very least, it should be the number of languages spoken across the immediate security risks. The private sector releases some of that pressure and given that an émigré, asylum-seeking, or refugee population often parallels such immediate security risks several alternative sources to the closed intelligence community could be made available if appropriate security arrangements were fashioned. Again, as background to the research, some effort to address this challenge was observed. Indeed, there has been some public effort by the intelligence community to recruit a broader ethnic mix.
- **Technical infrastructure weaknesses**. The blight of an impotent IT system seems endemic to public sector bureaucracies. Professor Simon Rogerson, Director of the Centre for Computing and Social Responsibility at the UK's de Montfort's University has publicly stated that: "All information systems fail".[55] A desire to develop bespoke systems is compounded by the requirements of security in the intelligence community. Yet, open source exploitation at least should be able to attract commercial-off-the-shelf

products given that, according to the US OSC estimate, at least 98 percent of their product remains at 'for official use only'.[56] The purpose of technical infrastructure is to facilitate the benefits of open source exploitation less constricted by compartmentalisation, security, or secrecy issues of closed - particularly communicability. The US Open Source Intelligence System (OSIS), an Internet-based password protected network, goes some way to achieving this. The additional challenge is 'mixing' classified with open at the desktop. Often, the only solution is a parallel system essentially resulting in two screens sitting on an analyst's desk with safeguards to prevent accidental (or deliberate) confusion. The technology arena is almost boundless. Data mining, geo-spatial tagging, data and geo-spatial merging, visualisation, filtering, machine translation and a host of others can and do contribute to the exploitation of open sources. Yet there is no standard or common system across or within intelligence communities.

- **Analytical capability**. As the number of perceived security risks grows, the breadth of expertise required beyond the traditional Cold War portfolio and indeed beyond the dominant terrorism threat no longer comfortably resides within the intelligence community. Again there is nothing new in the intelligence community co-opting specialists; but the challenge of knowing who knows has expanded beyond the simply national or specifically academic communities.
- **Validity/trust and quality control mechanisms**. It has already been mentioned that open sources are equated by some with the Internet and perceived as invalid *per se*. The intelligence community are not the only exploiters of open sources. Much work has been done to establish protocols for valid Internet presence, authority, and authenticity. Wikipedia is being migrated to 'custodian' and 'authored' product, whereby a panel of experts adjudicates each subject; and subject entries have to explicitly state the author's name for assurance and esteem for authenticity. This is very similar to grey literature open source product, where peer-review and citation statistics can contribute to judgements on expertise and therefore authenticity, validity and reliability.

- **Collective cognitive dissonance**. A cultural, organisational and conceptual resistance to the exploitation of open sources of information still persists, although the most senior intelligence practitioners, enquiries, and oversight committees express dismay at this resistance, and exhort increased open source exploitation effort.
- **Commercial approach**. Since many open sources of information, and expertise that can interpret it, best reside in the private sector, there is a need to adopt a commercial approach to its acquisition, which requires a business-oriented approach across the open source community if only for the sake of the taxpayer.
- **Information overload**. This is probably the most challenging aspect of the intelligence function let alone open source exploitation. While it is undoubtedly the case that information has expanded and is very unlikely ever to be surmounted, an attempt at its taming lies in three approaches: attitude, technology, and distribution:

    - **Attitudinal response.** The attitudinal response is based upon a just in time rather than a just in case approach to collection. This in turn necessitates a sharpening of the requirement stage arrived at between policy and intelligence communities so that the most pertinent questions are shaped before collection is embarked upon. Throughout the case-studies, this aspect was repeatedly noted by open source practitioners, who spent significant parts of their time in generating the appropriate question at the outset. In the case of ICTY, the open source cell simply dispatched 'customers' to do it themselves if they felt that they could and if question formulation would impinge upon their own research time. At SOCOM, the classic requirement question in need of refinement was "Tell me everything you know about Iraq"!
    - **Technological support**. The application of technology to data collection management is legion and of course explains why any intelligence function and certainly an open source function devotes resource to technology acquisition. The danger for any technological response to data management and manipulation is the propensity for reductionism and simplification, which is often seen in modelling and simulation solutions.[57] It is beyond the scope of this thesis to explore the more

specific impact of technology upon the intelligence function. Suffice to say that during the time span of this research the emergence of digitised 'mashing-up' techniques, social software, and machine language translation were observed being incorporated into the intelligence process.

- **Distributed intelligence.** Social software and the proliferation of user-generated content (principally blogs and wikis) have as yet unclear implications for all research-based information businesses. In the media world there is a notion that citizen reporting will be the death knell for journalism. In the academic community there is similar concern for the traditional peer-reviewed journal. For the intelligence community, the migration to the private sector of all things security is problematic. Again, the character and conduct of these institutions may very well be under pressure; even altered by these innovations. Yet, journalism, academia, and intelligence communities are already incorporating these new communication formats into the grammar of their respective professions.

The holy grail of open source exploitation might be represented in the notion of 'distributed intelligence'. Essentially, it connotes a sense that 'everyone' who is digitally networked and connected can be brought to bear upon a risk, perceived or otherwise.[58] More usefully perhaps, people who are recognised as 'specialist' or 'expert' can be brought to bear upon a risk more easily than ever before. The 'break-out' of Iraqi documents in 2005 onto the Internet for linguists to interpret (literally and analytically) is a good example of what might be achieved by the distribution of the intelligence effort. This 'wisdom of crowds', 'smart mobs', 'an army of Davids', 'blogswarming' or 'social search' is easily exploitable in the contemporary ICT environment.[59] Furthermore, such experts may prove more adept at pattern recognition in matters of human complexity than the claims of modelling and complexity science.[60] The hard work will be in identifying the experts. Of course there will always be 'secrets' or intentions that require a minimum of protection. However, that minimum is increasingly shrinking as the spirit of openness increases.

Deliberative judgement versus populist causes

Regrettably, it is not always expertise or specialism that is brought to bear upon a risk. It is just as likely that vested interest, personal gratification, populist culture, or sheer ignorance, amongst the panoply of human frailties, are launched at risk issues. The munificence and wonder of the Internet, the World Wide Web and instant global communication should not detract us from critical appraisal, argument and debate over principles, ideas and values in the formation of policy. In this regard, politics remains just as susceptible to the deep evolutionary tides of human strengths and weaknesses, emotion and logic, that have characterised decision-making throughout the ages. However, the contemporary transformation in ICT, when set against the context of the more recent social malaise broadly characterised by a lack of politics, presents an opportunity for populist processes to triumph over deliberative. The culture of celebrity and reality television may represent democratising processes in action, but the most votes cast does not necessarily mean that the best argument has prevailed. The need for wise judgement in the cause of human progress remains paramount. The underpinning principles that should secure 'preferred supplier' status are to be found in the very nature and fundamental purpose of their respective activities - why they do them not how they do them. In their own respective ways they all pursue truth - the best possible representation of reality - for their own purposes. In objectively critical but ultimately wise societies, where democratic deliberation trumps populism, demonstrating competency, outcome, purpose, and principle should be the normal measures by which society can decide where to place trust in its purveyors of reality. This rather depends upon the purveyors creating trustworthy environments, and societies retaining the faculties by which to decide. The context in which intelligence finds itself has broadened and morphed considerably since the Cold War. The context is shaping the conduct of intelligence as well as forming its largest target.

5.2 Part Two: Contextual Significance

> "… The posts come tiring on,
> And not a man of them brings other news
> Than they have learn'd of me: from Rumour's tongues
> They bring smooth comforts false, worse than true wrongs."
> William Shakespeare, Henry IV, Part II, Induction, 1597[61]

The exploitation of open sources transcends the operational. Because data can be created, collated, processed, analysed and judged for the purposes of deriving information, knowledge, or wisdom for humans, it is ultimately socially and culturally constructed. Because that knowledge can be globally transmitted and made virtually universally available, it contributes to the conduct of politics and the shaping of context in which we all operate. Any organisation, but certainly an intelligence organisation, needs to understand that context if it is to fulfil its obligation of telling truth to power.

All organisations are to one degree or another involved in the information business. Similarly, all organisations pursue the distinctly human characteristic of planning for the future. In this linkage they are also engaged in the risk business, which is explicitly concerned with being informed about the likelihood of future consequences. The intelligence community is definitively involved with the information business and implicitly, if not explicitly engaged in managing risk. It seems intuitive that information freely available in the public domain would be harvested rapaciously by an organisation whose principle input and output is information in one form or another. Because it is there, because they can, and because it forms 80 percent of final intelligence product, seems like an open and shut case for exploiting open sources. Not so! Significant cultural and structural barriers militate against any true representation of its effectiveness.

There is nothing special about open source information if one is objectively detached from the intelligence function. Equally, there is nothing special about 'closed' information if one is similarly objective. Yet, they are not treated the same. Their distinct internal characteristics and relative subjective comparisons mark out their value to customers, more

than their respective contribution to meaningful outcomes established by political masters with purposeful ends. Effectiveness ends with the customer's evaluation. Yet, because of its more holistic treatment of reality, open source can not only contribute to operational requirements, but it can also question whether the customer's purpose is valid at all.

5.2.1 Transcending operational: Nature versus character

Scientific advances have always been exploited, including for the conduct of intelligence. Both the use of telegraph by the 1850s and radio in the early twentieth century were technological developments that contributed to the changing character of warfare. Their encryption, interception, and decryption quickly led to the subsequent discipline of signals intelligence and information operations generally. The development of satellites in the 1950s led to the deployment of space-based platforms capable of collecting data across the electro-magnetic spectrum, notably imagery intelligence. More recently, seismography, forensic science and telemetry have contributed to the development of 'measurements and signatures' intelligence. Indeed, thanks in part to technology, war and its servant intelligence now inhabit the dimensions of land, sea, air, space and cyberspace.[62]

A key shift occurred with the invention of electricity. A geographical and temporal distinction, between intelligence conducted prior to the invention of electricity and post electricity, significantly extended the 'range' of operational intelligence from less than a hundred miles and a matter of hours to its global and instantaneous range today.[63] The last 150 years of technology, incorporating electricity, has seen a qualitative step change in the character of intelligence, as different as the 1,500 years before was constant and dominated by the speed of foot, horse, sail and line of sight.

Of course, it might also be suggested that the invention of the alphabet, the printing press, and the railway, amongst others, could claim similar step changes in the information business and thus significant shifts in intelligence affairs. However pretentious or accurate their respective claims, perhaps the more important point might be made that, while the

character of intelligence may indeed have been altered dramatically by these technological developments, the nature or purpose of intelligence was not. Indeed, given the historical evidence, one might confidently suggest that future technological development will change its character and conduct still further. Yet, the nature and purpose of intelligence - support to decision-making - will likely remain constant, however it is conducted.

The technological innovation of contemporary times, itself a development of electricity and an understanding of the electromagnetic spectrum, is digitisation combined with information and communication technologies (ICT). The shift that it brings is not just qualitative but also quantitative. The availability of virtually unlimited data and sources, in what is euphemistically called the 'information age', is difficult to comprehend let alone tackle. New attitudes to collection (just in time rather than just in case), new information processing techniques (data mining algorithms, visualisation software), and distributed forms of analysis (social software) are emerging to cope. Furthermore, thanks to the Internet, the World Wide Web, satellites, and mobile telephones, this information - the same information - is available to anyone equipped with a personal computer and an appropriate connection (see note 48 to this chapter). However, whether this democratisation of information merely deepens cultural relativism or furthers a genuine universalism of 'best truth' remains to be seen.

Again, the intelligence community, amongst other research and analysis hungry communities, has not been slow to recognise the opportunity afforded by the exploitation of these publicly and openly available sources of information; albeit with mixed implementation records. Of course, the exploitation of open source is not, of itself, new, although the scale and availability are. To stress the distinction between nature and character; the character of information exploitation is changing dramatically as a result of the latest transformation in ICT. Its purpose is not.

Yet, technology alone does not determine context. Technology allows us to interrogate context while simultaneously shaping the context we want to understand. Furthermore,

cultural and social forces are also important. While shifts in information and communication technology are tangible and easily observed, changes in socially constructed context are more insidious. Political will, an entirely human affair in the design of strategy, remains the key influence upon the dance of relative power between nation-states and other entities that forms our geo-political context.

Moreover, contemporary technological change and socio-cultural change seem connected. Ideas and information can travel the globe, less limited by the difference between developing or developed nation status, than by the 'digital divide' and the capacity for intelligent reception by its audiences. Whether those ideas are valid and universal, or such information might be assessed as useful knowledge, remain timeless questions of principle subject to the application of those who purport to be executors of wise judgement. And it is not just that a single context is changing; several parallel versions of context are discernible. Two seem pertinent: the context associated with western nation-states' interests 'abroad'; and the context for western nation states at home.

With regard to the significance of context to intelligence, Aldrich argues that globalisation rather than terrorism is what intelligence agencies should principally focus upon.[64] This is also to point out a distinction between context and operations. Understanding the impact of globalisation is the bigger challenge than an undisputed operational necessity of managing a species of criminal.[65] The former is subtle and contentiously defined. The latter is material and more easily grasped. Alongside globalisation, this thesis has introduced the notion of 'risk society' as an influential shaper of contemporary context - troublingly so.

5.2.2 Risk: Its influence on context

> "At least at the strategic level, we need a national intelligence system where we are less concerned about betrayal from within, and more focused on emerging strategic threats to our long-term security and prosperity, threats that must not be limited to man-made capabilities, but include animal borne

> diseases and other environmental conditions that tend to be shut out from national security decision processes."
>
> Robert D. Steele, 2006[66]

The misunderstanding of context manifests itself most notably in another contemporary and contextually shaping phenomenon alongside globalisation - the phenomenon of risk - in which intelligence implicitly if not explicitly deals.

The management of risk has migrated from the actuarial-based statistics of 18th century merchant shipping insurance, through corporate governance guidelines in response to the financial scandals of the early 1980s, to the ineluctable and pervasive concept that it is the means by which future uncertainty can be predicted, measured and controlled. How did uncertainty miraculously become knowable and, still worse, become 'measurable' and 'modelable'? Because it is given a number, pseudo-meaningful in the contemporary positivist rational actor paradigm, it becomes dangerous simplification and reductionism than any increase in understanding.[67] If metrics are to be applied to abstract phenomena like intelligence outcomes, to make their effectiveness measurable, then it may only be appropriate at an operational level and only then in the presence of a denominator, for example successes divided by failures.[68]

A causal-attributive approach to simple or complicated challenges, such as Cold War technical intelligence collection of types and numbers of equipment, is no longer dominant - if it ever was.[69] In a complex or chaotic (rather than merely complicated) world, complex-adaptive approaches to decision-making in conditions of uncertainty are more appropriate. Holistic narrative understanding of context based upon pattern recognition becomes more useful to wise judgement than 'black and white' analytically structured decision-making based upon linear data processing.[70]

Risk management, inextricably but misleadingly linked with uncertainty, has come to transfix governments and institutions alike with a powerful, hypnotic reason for being. It is as though the very word uncertainty has been stripped of its original dictionary meaning.

When connoted with risk - merely by linking it to institutional objectives and developing procedures that ostensibly do no more than manage the management of risk - the management of uncertainty becomes endowed with senses of control, strategy, and solution.[71] The effort to manage uncertainty becomes an organising concept in itself and devoid of any higher meaningful outcome.[72] Thus, the reason for being becomes - similar to the interchange of purpose and process - the management of risk as organising principle in its own right.[73]

Consequently, the employment of 'business continuity' practitioners, 'risk assessors', and 'reputation managers' reflect, not so much the value they offer *towards* achieving institutional objectives, but their establishment *as* principal objectives. The consequences of the primary work *of* institutions - what they do - have been traduced for the management of potential secondary risks *to* institutions - what may or may not befall them. That is to say their reputations have become more important than achieving their objectives, when the achievement of objectives is what traditionally created reputations. Similarly, business continuity assumes equal significance to the conduct of business.

One hopes that institutions do not confuse ends and means deliberately, as some sort of control exercise. That would at least be wilful. It is that contemporary social constructs - disengaged politics, disaggregated societies, a disbelief in science, and diverse philosophical principles - have created an unmediated, unchallenged, relativist environment. Thus, institutions sleepwalk into a systemic, pervasive mindset that justifies their activity, when, in effect, all they are doing is substituting the pursuit of meaningful outcomes with process and 'performativity'.

This bureaucratic decline into mediocrity is being pursued across many institutions and disciplines. Barnett highlights it in the epistemological and sociological undermining of latter-day higher education.[74] Tallis challenges the re-interpretation of league-tables and waiting-lists as narrative for what it once meant to be well in the health service.[75] Power and Hunt both articulate the notion of 'the risk management of everything' within the

commercial world in the sense that formerly straightforward internally-facing corporate control mechanisms now guard externally against reputational risk.[76] Saatchi delivers a withering critique of Anglo-American pragmatic politics too frightened to exhort anything remotely ideological.[77] And there is a plethora of literature that questions the socially ingrained logic of Beck's risk society thesis and its supporting 'runaway world' protagonists.[78] This risk society logic is a logic in which science and technology have somehow become reflexively responsible for our future demise as a species, forgetting that science and technology have determinedly delivered much of what is deemed 'progress' today, and might continue to do so in the future.[79] There is nothing essentially new in Beck's analysis of an ultimately and inevitably degenerative society. Plato's *Republic* beat him to it by nearly 2,500 years.[80] Yet, we are still here!

In many aspects of life the progress of science and technology over the last 100 years - medicine, education, communication, and living standards - has been extraordinarily positive and beneficial, if not universal. Undoubtedly, new risks have emerged, and the perceptions of some of the consequences of these new risk sources - GM food, nanotechnology, artificial intelligence, climate change, and globalisation - can be ambiguous and alarming. However, it is worth remembering that some of these so-called new risks have been with us for a very long time. Piracy and the slave trade are very old examples of transnational crime. Crops have always been manipulated to improve productivity; today it is has simply become more clinical and precise. We have always managed to adapt to, and exploit, climate change. Furthermore, some risks like smallpox have been eradicated, poliomyelitis and Dracunculisasis nearly so, while once deadly diphtheria, tuberculosis, whooping cough, Scarlatina and typhoid fever have been greatly reduced through immunisation programmes and antibiotics. Essentially, these new risks are merely new to us, relatively no less challenging than their predecessors were to our predecessors; perhaps less so. What seems dangerously new is a misanthropic unwillingness to meet them.

To confuse risk for uncertainty is mistaken. To conflate the source of a risk with its possible consequences is disingenuous. To equate the perception of a risk with its reality is disabling.[81] To equate the reality of risk with potential consequences absent of human intervention is to deny resilience and a wilful purpose to genuinely manage risk. To invoke the precautionary principle as reaction to potentially detrimental consequences is to also deny the benefits of potential progress, itself an irrational and incoherent precaution.[82]

The differentiation between the reality of a risk and its perception has been recognised in a much wider body of literature (Chapter Two: 2.2.2). But, just using the most simple risk analysis technique - likelihood-impact analysis - it can be empirically demonstrated that it remains 'safer' to fly than to drive to an airport to catch a plane.[83] In the same vein, a whole range of contemporary moral panics, including terrorism, attract the scorn of risk theorists, as they seem to 'fill the frame' of commentators and snake-oil salesmen that live off the back of them. Mobile phones, flu pandemics, obesity, animal rights, and GM technologies are just a few, that incur a precautionary reaction as default. This reaction has much more to say about the fragility of contemporary society, largely western, as it seems beholden to notions of victimhood, rather than the exercise of wise judgement.

Here the intelligence community have an opportunity to correct or reset the apparent existential crisis of contemporary western society by contributing a better truth to be put to power - in this case society and its changing societal expectation - than we seem to be currently presented with. Specifically, the exploitation of open source of information together with an analysis methodology that incorporates the best thinking of risk theory might go some way to achieving this. Such thinking attempts to combine both an empirical as well as human factors approach. It recognises that it is insufficient to understand a hazard or threat alone; it has become clear that an understanding of how the risk of a hazard or threat is transmitted as perception is also crucially important. This all has implications for the prioritisation of effort and the allocation of finite resources - a policy matter.

The really debilitating effect is not the explosion in risk, but the explosion in everything being interpreted as risk.[84] Absent of meaningful objectives, values, and principles, western society is increasingly and mistakenly utilising the management of risk as ends rather than means to ends. In this process, institutions are turned inside out, the marginal risk becomes normalised while the normal risk becomes marginalised, and the management of risk, once a by-product of organisational endeavour, becomes organisational principal.[85] The crisis advocated in the central thesis of risk society ought not to be the imminent demise of society at the hands of malevolent scientific and technological progress; rather that a crisis exists in the absence of purpose to put such technological progress towards.

Furthermore, the management of risk is a zero-sum game. That is to say, a course of action 'wins' or is implemented at the expense of another that 'loses' or is rejected. It comes with costs, choices, and the allocation of finite resource. When China pledges $1.9 billion to fight 'avian flu'; this may be perceived as a benefit in the management of the risk of avian flu, but it comes with a cost, and, seemingly, absent any evidential-based prioritisation. Avian-flu has killed some 100-plus people worldwide to date. Malaria, a genuine risk and preventable disease, claims approximately 3,000 deaths every day in Africa, and requires $3 billion every year to control. The allocation of $1.9 billion to avian-flu may be responsible for a further decline in support to the already sub-optimal $600 million that malaria received for 2005.[86]

Similarly, the pursuit of the 'what-if' or the 'not if but when' of risk is a dangerous game. It conflates what should be private with what should be public by pandering to the demands for accountability and transparency as though these of themselves make risks diminish.[87] The failure of imagination described by the US WMD Commission in 2004 is the unedifying but singular prerogative of intelligence communities, not the public.[88] Rather than managing the reputation of their community - secondary risk - intelligence organisations should engage in private internal substantive performance change to aid their primary work. They in turn should be informed by the best possible information sources. These are unlikely to reside solely in the closed intelligence world. Yet it may be the

intelligence community that is best placed to coordinate the best possible truth on so-called 'new' risks by knowing who knows. The Better Regulation Commission outlines a similar and parallel recognition of the wider use of information sources to inform the management of risk within context, although they stop short of security risks.[89] Interestingly, and perhaps taking lessons from the intelligence community, they recommend the establishment of the Fast Assessment of Regulatory Options (FARO) Panel, which might loosely be compared to the UK's Joint Intelligence Committee.[90]

Ironically, there is a very great danger that an increase in imagination might actually exacerbate the zero-sum and what-if dilemmas rather than make us any more secure. Where we spend finite resource should be decided by hard evidence rather than a surfeit of imagination. Knee-jerk reactions combined with a desire to be seen to be doing something are fear-based responses not rational ones. In the absence of hard evidence - uncertainty - to support risk management techniques, wise judgement based upon cost-benefit analysis should prevail over any pseudo-science. Alongside the notion of intelligence failure are being placed equally convenient lapses in intellectual rigour denoted by phrases like 'joining the dots', 'groupthink', or 'beyond normal comprehension' as explanations of intelligence failure. This is particularly true of the contemporary analysis of 'new' terrorism. Yet, the true failure of intelligence with regard to both 9/11, and particularly the Iraqi WMD débâcle, is not so much the failure of analysis or the manipulation of intelligence product, but that there was virtually no intelligence either for intelligence analysts to interpret rationally or for politicians to manipulate maliciously.[91]

Aldrich, among a very few writing about intelligence, has recognised the potential folly of the intelligence and security community concentrating upon the latter day 'new-terrorism' to the exclusion of all other matters.[92] Encouragingly, there are some extremely senior intelligence practitioners within the UK IC, who also recognise the dangers: "We concentrate too much on counter-terrorism, plus Iraq and Afghanistan, which means other targets are left exposed".[93] In particular, Aldrich notes the contemporary version of globalisation - there have been several historical variants - as being a more worthy target of

the intelligence community than terrorism. He argues that it is globalisation - the decreasing importance of territory - that is the conduit for contemporary threats. Others have specified the threats that globalisation enhances; most notably Rischard and the intelligence community themselves.[94] Of course others, while recognising today's version of globalisation, do not see the impending demise of the nation state given the absence of any alternative form of global government.[95] Nevertheless, the pressure on borders and the traditional choke points of interest for intelligence and security officials works against them rather than for them. Additionally, the ICT transformation that is the engine of globalisation seems to choke the intelligence and security community with a surfeit of data that cannot be processed let alone collected efficiently.

The inability to understand terrorism is no more than the anxiety of being unable to convincingly translate it into something that matches the deep ideological preconceptions that have characterised modern clashes, 20th Century at least, between liberal democratic systems and authoritarian ones. Furthermore, all of this institutional anxiety is being transferred to a whole range of new risks characterised by uncertainty, more than the traditional quantitative properties of risk, and set before intelligence communities to comment upon as though their analysts have suddenly become endowed with divine prophecy. Understanding that a risk may actually not be understandable, because it simply does not have any meaning substantiated by evidence, is an objective that open source exploitation is more likely to achieve. This does rather beg the question in the contemporary world of new risks: what does closed intelligence contribute?

To make matters worse, the anxiety of non-understanding is also conquering the personal realm as authenticity of personal goals and meaningful lives are replaced by superficiality.[96] The risk of 'the risk management of everything' phenomenon is reinforced, publicly at least, by a mood of cynicism, which rejects discussion and debate about whether these new risks are any more risky than those faced down in the past. Perceptions of risk tend to be formed more out of fear and dread than by rational means.[97] Conversely, realities of risk are informed by an assessment of their likelihood and impact

and then reassessed following the imposition of risk management treatments. Debates about 'intelligent design', animal rights, lifestyle choices, genetic modification, and even the search for the Higgs Bosun, to list a few, take on deeply misanthropic and unconfident value sets absent this rational approach.[98] Cynicism replaces scepticism, caution becomes precaution, risk aversion eradicates risk taking, victimhood trumps heroism, regulation precedes cost-benefit analysis, and stagnation suppresses progress. The greatest tragedy in contemporary western life is to be found precisely in this societal floundering that occurs in the growing gap between perception and reality. Perhaps the intelligence community's greatest contribution in this climate might be to help steer society out of it. Gill and Phythian came to a strikingly similar conclusion in late 2006:[99]

> "Citizens have been excluded for too long from any knowledge of intelligence policies and practices, but now live in societies in which security fears apparently increase relentlessly. One important task for researchers is to make sense of and communicate the extent to which fears are well founded and how far they are manufactured."

It is only with the great healing of a decent passage of time after apparently momentous events that one might begin to question this culturally engrained notion of a risk obsessed society that unquestioningly sees security as the 'new infinity'.

Thus, Steele, quoted at the start of this section, has it only half right. The implication in his declaration, acculturated and endorsed by his prolific reading list (notably Rischard's High Noon[100]), is that there are other threats that we need to 'worry about' beyond mere security. He inadvertently or otherwise recognises that risk is the common thread, the progenitor of security, natural disaster, health, safety, and other risk classes. However, he reveals a common tendency in contemporary society to unquestioningly support the need for management of such risks without first critically assessing their legitimacy in the first place. It is not that these hazards, threats or natural phenomena do not exist; but it is whether the level of risk they constitute has been accurately assessed. To convert them directly into the need for a regulatory policy avoids the difficult and necessary intervening steps associated with risk management. To assume the worst is - to use intelligence

parlance - not so much a failure of imagination but an exuberance of imagination absent of evidence. Popper put it succinctly:[101]

> "Such arguments may sound plausible enough. But plausibility is not a reliable guide in such matters. In fact, one should not enter into a discussion of these specious arguments before having considered the following question of method: Is it within the power of any social science to make such sweeping historical prophecies? Can we expect to get more than the irresponsible reply of the soothsayer if we ask a man what the future has in store for mankind?"

This is where the author considers that open source has a benefit beyond the simple characteristic of information source. It is the exploitation of open source, which may allow more of us to critically question the underlying assumptions of received policy. This plays back into the notion of a changing societal expectation. The exploitation of open source may question the very necessity for a risk management strategy to be effected at all.

Thus, the very important issue of balanced intelligence budgets - whether we are correctly apportioning open to closed expenditure based upon the 80 percent efficiency rule - is now subsumed by an even greater debate about the relative expenditure on regulation across all risk classes. In a climate of politics characterised variously as fearful or managerial, the very objectives of society can be shaped by the decision support offered by the exploitation of open sources by many more of us. All that is needed are more robust ways of expressing it.

Manunta provides a definition of security that is useful at the operational level: security is a relationship between 'assets', 'threats' and 'counter-measures' (he uses the word 'protection' for counter-measures).[102] If any one of these three is not present then a security situation does not exist. Both the definition and observation highlight the distinction necessary between context and operations for intelligence. The role of the intelligence community at an operational level is, in the very broadest sense, to 'deal' with threats through the imposition of counter-measures. At the contextual level, globalisation, *qua* security, cannot easily be assigned as an objective of the intelligence and security

community. Globalisation represents both threat and opportunity quite apart from the fact that as an abstract noun it remains as problematic as terrorism to treat as the source of a security risk.

However in the contextual sense it seems perfectly reasonable that the intelligence and security community should at least understand globalisation as a key driver of contemporary society. For example, Aldrich argues further that globalisation is not merely a simple choice between liberty and security but additionally a three-way balance between liberty, security, and 'luxury'. Luxury might represent both the enormous progress of western society as well as the imbalance of global resource consumption. This becomes a very difficult relationship for governments to balance let alone intelligence communities to 'deal' with. In their effort to do so, and in common with other, and similar, problematic risks that are characterised by high impact low likelihood designations, they collectively resort to the precautionary or pre-emptive principle in order to be seen to be acting as exercisers of power than executors of rational judgements based upon cost-benefit analysis or even a sense of libertarian paternalism.[103] Aldrich's argument suggests that in this irrational climate of decision-making, characterised by the need to appear transparent, the intelligence agencies have themselves become victims of politicians' irrationality, if not their 'fall-guys'.[104]

The greatest challenge for intelligence at the contextual level is not new terrorism or indeed any other of the apparent perceptions of risk. Rather, it is in identifying what the purpose of our society should be in contemporary times, now that the ideological struggle between the Cold War protagonists is largely over. The exploitation of open sources in all its forms can contribute at this level and in two other regards. First, that, as the thrust of this thesis has shown, open source exploitation at an operational level provides a significant amount of the final intelligence product devoted to dealing with threats at this level. This research shows precisely how it contributes. However, second, an additional consequence of the research has been to highlight a more deeply fundamental and philosophical nature to the purpose of information; namely the understanding of context combined with the provision

of best truth on matters of risk in order to avoid the debilitating effect of applying the precautionary principle. Thus, open source exploitation is not just about the collection and analysis of information for operational purposes. It is also about 'open thinking' in that it can be used to contribute to more open debate by exposing the myths that are too easily created in the contemporary socially narcissistic and solipsistic digital media world. Furthermore, it can inform policy that is either mistakenly advised to suit the 'pigeon-hole' heuristic (our preconceptions) or wilfully politicised to suit power. As Ross puts it:[105]

> "We selected facts … which suited our version of events. … (T)hose we met told us, in general, what we wanted to hear. … The common thread of these missteps is that policies are decided by small groups of officials and ministers based upon very partial (in both senses of the word) accounts of reality, abstractions several removes from the facts."

5.2.3 A crisis of confidence: Means and ends inverted

That knowledge might transform society ultimately depends upon society showing purpose for its own existence in the first place.[106] Knowing where it wants to go and what it wants to be - a sense of purpose - takes precedence over how it is going to get there. 'Getting there' is where intelligence, in the sense of support to decision and policy-makers, ordinarily resides. And 'there' should be determined through wilful politics generated by a debate over ideas and values, delivered by politicians through the exercise of power invested in them by citizens. Yet, today, western polities, particularly Anglo-Saxon ones, seem unable to express a vision of where they want to be or what they stand for.[107] This quest for purpose is further compounded by not truly recognising where they are starting from. Rather, they act reactively or pre-emptively, thereby illustrating only what they are against.[108]

The response to terrorism post 9/11 is a case in point. Western societies have been complicit in placing so-called 'Jihadi' terrorism upon a pedestal it does not deserve.[109] The reality of terrorism, all terrorism, is that it is an irregular mode of warfare for political purposes. It is not strategy of itself.[110] The pseudo-ideology of this present violent

expression of extremism is essentially nihilistic and devoid of meaningful, certainly achievable, politics.[111] Yet, considerable resources of the state are being thrown against it as though it represented an all-consuming political challenge to what we believe in, when it is we that have endowed it with any notion of political sense and the strategic significance of war. It is a strategic and ideological mis-match of our own making that should be dealt with by the proportionate and operational means with which we treat any criminal. Meanwhile, the values and principles that have underpinned our strategy and ideology, heretofore, seem increasingly marginalised and ineffective. It is worth noting that the then UK Prime Minister (Blair) thought precisely the opposite: the ideological struggle is absolutely strategic. However, he also thinks that values are the key - albeit exercised through progressive pre-emption.[112]

The battle of ideologies, if there is one, is conceived and perceived to be with dysfunctional factions of Islam, but perhaps the war of real political significance is internal to the West and with itself.[113] Compounding this absence of the establishment of meaningful objectives, or 'ends', is a politics of managerialism that merely results in 'means to ends' becoming ends in themselves. Polities identify the 'threats' and promise to manage their risk on our behalf in exchange for power. However, the management of these risks becomes purpose in the absence of purposeful vision and goals for society. As means and ends become confused and interchangeable, purpose is replaced by process masquerading as purpose.

Part of that confusion derives from a misunderstanding or misreading of context. If context is misunderstood then purpose will be equally misguided. If purpose is misguided, then many institutions, not least intelligence, are similarly blown off course in the operational conduct of their business. To paraphrase Gray: it is important that leaders get the big things right; everything else will follow.[114]

Yet, politicians and politics on both sides of the Atlantic (at least) seem to flounder when it comes to articulating purpose, values, and principles. Indeed, it may not be just politicians

engaged in a frustrating search for meaning. The middle-class, British-born, relatively well-off, young, male suicide bombers that brought carnage to London in July 2005 may very well have claimed (mistakenly) a pious devotion to Islam; but their acts could equally be interpreted as being motivated by a nihilistic sense of 'lashing-out' at a society that gives them no sense of purpose or identity; curiously unlike their 'first generation' parents.[115] The wearing of veils (crucifixes, or any such external symbolism) might similarly be viewed as a desire to belong or as a need for meaning in societies that decreasingly offer these things beyond the celebration of self, celebrity, and the individual. It seems ironic if not hypocritical, for example, that we condemn acts of depravity in our running of prisons abroad, when similar acts can be witnessed at home on so-called reality-TV. Furthermore, this need for meaning is not exclusively ethno-centric or religious. It can be found in the environmental movement, animal rights activism, anti-war protests, and anti-Americanism sentiment. They all display a profound lack of confidence in western values; and they are home-grown. The danger is that arcane belief systems, religious to environmentalist, together with an unrivalled media, become persuasive ideology because there is nothing to challenge or temper them.

When means are misinterpreted as ends, and institutions seem absent a sense of purpose, one might interpret that as evidence of the emergence of an existential crisis of confidence. Some might balk at this assumption. Indeed, it may very well be - similar to new risks - more in the perception than the reality. In the same way that the fall of the Berlin Wall in 1989 is often described as 'world-changing', so too are the tragic events of 9/11. Yet, 1989 and 9/11 were culminating events - dénouements - signposts of an already changed context influenced by the historical narrative that preceded them, rather than points of origin for new narratives. It seems no coincidence that this crisis of confidence was exposed in 2001, not just by 9/11, but by the triple impact of the 'dot-com' bubble bursting, the Enron scandal, and 9/11 combined.[116] It is we that turn them into new departure points rather than ends of old stories (more so after 9/11 than 1989 curiously), and then compound the misunderstanding of context further by converting them into things we are against as new purpose.

5.2.4 Open source exploitation: Intelligence theory, knowledge and power

> "Both of us, governors and governed, rely on an easy myth, a piece of theatre. This is that governments, in the form of foreign ministries and diplomats, understand the world, can interpret its signs and correctly formulate policy in response. This is an illusion."
>
> Carne Ross, 2007[117]

With regard to the current evolution in intelligence affairs, two things seem pertinent. First, there is some recognition that the intelligence business today is about the total information business.[118] Warner's definition of intelligence - secret state activity to understand or influence foreign entities - has come to define both the character and nature of intelligence. Yet, with regard to character, it seems more a definition of intelligence as espionage (process) than intelligence as knowledge (product), whether practised by Sun Tzu or in the highly secretive Cold War environment.[119] With regard to the underlying nature of intelligence, it only partially addresses purpose in any strategic or contextual sense.[120] It does not answer the question: why do we want to understand or influence foreign entities? In other words, to what ends of our own? Second, that the effectiveness of intelligence cannot be measured or conducted in some sort of pseudo-scientific, positivist, quantitative, managerial way; rather it remains an art servicing best judgement, validated by how it 'makes a difference', and how that difference is ultimately 'measured' as in judged against society's objectives.

Intelligence can either do the more important thing of working in support of those objectives or become trapped by the conventional 'managerialism' of our time. Yet, establishing society's objectives is not the purpose of the intelligence community. That is the purpose of willful polities engaged in meaningful debate over ideas and principles. Unfortunately, this is precisely where the gap lies. Perhaps that should not prevent the intelligence community from acting as if those objectives were in place or better still informing their construction. The balance is a delicate one. How should 'power' debate and decide objectives without information? Or, in other words, who has the responsibility for informing power, and about what?

Thus, the place, or a theory, of intelligence in the relationship between intelligence and power in contemporary society is 'up for grabs'. If one agrees with the classical definition of intelligence described by Warner then, as Gill and Phythian explain, it merely becomes a metaphor for surveillance; where knowledge is represented by data collection and power is the exercise of control via supervision, regulation, and risk management.[121] However, if one agrees with the notion that intelligence today is something more than espionage or covert activity then it is about understanding the best representation of reality in order to support decision-making for purposeful objectives. This will require a substantial exploitation of open sources; not just in the informational sense, but in a broader sense of open software, open spectrum and open communication.[122]

Here, the crisis at the heart of politics, crucial to the role of intelligence, might be differentiated from a wider societal one. Politicians seem increasingly afraid to debate issues, decline to stand or fall on their convictions, and are fearful of 'leaks' about anything they say. Consequently, they 'cabal-up'; concentrating power in ever reducing circles.[123] By way of a sop, and exemplifying the politics of managerialism, they submit themselves and other institutions like the intelligence community to accountability, oversight and transparency regimes that in turn seem powerless to act meaningfully upon what they hear.[124] The post 9/11 recommendations or the issue of rendition seem good cases in point.[125] Subjecting institutions to compliance procedures removes them from deliberative, political, even ideological judgments. It is this dangerous flight from wise judgment toward defensive compliance, defendable procedural structures, and the management of reputational risk that is our biggest risk.[126]

As Onora O'Neil suggests, transparency, accountability and oversight mechanisms may reduce secrecy but they do very little for deception and the creation of trust.[127] Whether intelligence conducts its work in public or private matters not a jot. Whether they are trusted to achieve their objectives is more important. Thus, she suggests: secrecy is not the enemy of trust - deception is the enemy of trust.[128] No amount of transparency or accountability will trump meaningful outcomes.

Here, Steele falls into the utopian trap and contemporary malaise that views compliance as ends in itself, when he posits that: 'The U.S. taxpaying public desperately needs a collective intelligence agency (cia) (*sic*) that can collect, process, analyze, and disseminate truthful information about the real world *to the citizen-taxpayers so that they can hold their government officials, and their private sector providers, accountable* (emphasis added).'[129] Steele's argument seems correct until the emphasised italics. However, orienting open source exploitation towards accountability and compliance mechanisms (particularly the present excess of it[130]) rather than any greater societal purpose is precisely the problem. It creates a pseudo trust, a blind faith in procedure, and an organisational rallying point that usurps primary work in support *of* objectives, for the management of secondary, reputational risk *as* objective. The danger lies not only in the vacuum left by an absence of purpose, but also in filling the vacuum with an equally vacuous mantra of accountability, transparency, and managerialism rather than ideas, principles and values. Filling the void with the organisational principle of risk management, an otherwise acceptable by-product of good management control, is simply replacing one hole with another.

This externalizing of once straightforward internal by-products of control into reasons for being *is* the crisis. It manifests as regulation, governance, excessive legislation, political correctness, diversity, and an unhealthy obsession with quantification - amongst others - all in an attempt to control the uncertain and, by implication, unknowable. These are all eminently worthy tools to protect, pursue, prevent and prepare, but not ends in themselves. Indeed, these tools are specious in the absence of knowing what they are trying to support. Simple measurable targets seem to have replaced the more difficult wise judgment.

5.3 Summary

> "Although only a few may originate a policy, we are all able to judge it."
> Pericles of Athens, ~430 BC[131]

The recent RAND/DNI workshop on intelligence reform - 'Towards a Theory of Intelligence' - reflects just how fundamentally challenged the role of intelligence is in

western societies today. That it should recommend a return to first principles and interrogate the very purpose of intelligence is both commendable and alarming.

This section has explored the distinction between the nature of intelligence, what it is for, from the character of intelligence, how it is conducted. It argues that the nature or purpose of intelligence has not changed - support to decision-making; truth to power; or who knows what, in sufficient time, to make use of it - all remain extant. Indeed, the author has argued that there is little new under the sun as far as the nature, *qua* purpose, of intelligence is concerned. By contrast, it has been argued that the character or conduct of intelligence is continually evolving commensurate with the changing context in which it finds itself.

Part of that changing context is a step-change in the volume and availability of public information afforded by the latest transformation in information and communication technologies. The discrete, formal, and deliberate conduct of open source exploitation for intelligence purposes reflects this. Yet, even in this latest manifestation, the character of intelligence continues to evolve as open source itself expands into 'open spectrum', 'open software', and 'new social media'.

At the time of completing this work, the awareness of open source intelligence as a phenomenon has gone 'public' and is becoming 'mainstream'. At the start of the research, the author received a single 'google-alert' per month on the subject of 'OSINT'. By mid 2006, the number of alerts had risen to several per day as both private information brokers openly publish their work based upon open source exploitation and the blogosphere picks up the subject. The tone of their content indicates first, a frustration with the traditional secret intelligence outcome and second, a sense that open source exploitation can 'save the day'. The former reflects a perpetual discussion amongst intelligence scholars and practitioners as to where intelligence failure (rarely success) resides. This is not a new argument and not within the scope of this thesis. Suffice to say that Betts treats it best when he points out that intelligence failure can also be a euphemism for policy

imperfection and, anyway, is inherently inevitable.[132] The latter, however hopeful and sincerely felt, is misguided.

At a purely operational level, the formal and deliberate exploitation of open source information, within all intelligence agencies supporting security, law enforcement, and defence communities, reflects the arrival and acceptance of open source intelligence product as a new information class alongside Humint or Techint. Meanwhile, the expansion into other open methods is shaping process. This chapter has detailed how open source exploitation contributes to the intelligence function: context; utility; cross-check; focus; surge; communicability; and analysis, and assessed some of the implications. Work remains to be done on the overarching policy, doctrine, and training for open source exploitation, and there is still debate to be had as to whether it should reside within or outside the established closed environment; but the intelligence community is well aware of its importance, and is integrating it.

It is worth emphasising that the most significant contribution of open source exploitation is at the contextual level, precisely because it reflects changing context and thus transcends the purely operational. Rather than just answering questions, it also shapes the questions that ought to be asked. It can provide the evidence to help challenge the fundamental assumptions of intelligence activity at the outset; the elusive but much sought after 'critical thinking' of all intellectual activity. Thus, this richer understanding of context has a more fundamental role in informing the purpose of intelligence than simply supporting its conduct.

This chapter has further argued that the justification for intelligence is efficacy not secrecy. Efficacy substantiates the enduring nature of intelligence; secrecy merely distinguishes its character. Whether strategic or operational objectives are achieved through closed or open means is immaterial. However, efficacy, distinguished from efficiency and effectiveness by its connection to objectives, remains difficult to demonstrate.

Beyond secrecy and further debilitating the demonstration of efficacy is the ideological grip of risk upon contemporary society. The deployment of the precautionary response to misguided notions of a reflexive risk society increasingly results in the formulation of knee-jerk rather than evidence-based policy. Furthermore, the misapplied positivist, quantitative, and mechanistic methods of risk management to issues of genuine uncertainty have supplanted wise judgement in pursuit of organisational objectives for process *as* organisational objective. The exploitation of open source to understand context might dissipate these effects through access to a wider evidence base, illuminating the reality of risk, as well as narrowing the gap between its perception and reality.

Finally, for context, this chapter has posited that a lack of self-confidence within western societies, particularly their polities, further endows risk with autonomy and fear that previous generations would have engaged with, rather than be paralysed by. Contemporary influences (by no means exclusive) - globalisation, changing societal expectation, and particularly the more pernicious notion of risk society - seem to create a crisis of confidence for western polities that has seen them struggle to articulate notions of what they are for while succumbing to easier expressions of what they are against. The downward spiral into form over content, means masquerading as ends, and the absence of any meaningful, ontological sense of security as outcome, is the consequence of a politics of purposelessness. This apparent vacuum at the heart of western polities feeds into and off the downside of contemporary influences. On the one hand, society, through politics, needs to (re)establish its purpose for contemporary times so that intelligence can contribute to achieving it. On the other hand, intelligence should avoid being drawn into supporting an 'easy' false context and strive to expose the much harder best-representation of reality. Perhaps intelligence faces a more fundamental paradox than revolution or reform - remembering what it is for.[133] Pericles seems to have been 'right' on so many levels!

Open source exploitation does not present us with a magic wand. The public awareness of open source intelligence is at least a decade behind its formal exploitation by public sector intelligence agencies. Yet, this exploitation has a mixed record. Some exploitation

efforts, such as the ASD and SOCOM in the US military and the agencies represented by the UK's SIA have survived and thrived, while EUROPOL, DIS and the VIC/APAN, by contrast, have struggled and suffered.[134] Furthermore, this research has indicated that, like any other class of intelligence activity, open source exploitation is subject to the same absolute and immutable information tests - validity, reliability, and timeliness. It is the subsequent interpretation of information in order to best represent reality and optimise decision-making that remains critical to human endeavour more so than its origin. More widely, the collection, interpretation and dissemination of open source exploitation broadly follow the same pathways around, and shortcuts across, the intelligence cycle as other intelligence discipline. Similarly also, at the transfer point between knowledge and power, the purpose of the provider and customer may be at variance. Yet at that point the intelligence job is done.

Relatively, open source exploitation has some distinct advantages compared to other information classes such as Techint or Humint, and the high order factors indicate where they may lie and how they might be prosecuted. However, none of these advantages of themselves demonstrate any increased efficacy for the intelligence function as a whole. They merely show why and how open source exploitation contributes to final intelligence product and is thus of value to its customers within a closed intelligence community. The '80-percent rule' exemplifies this. But, looking from the outside, this rule merely represents a measure of efficiency. Whether the exploitation of open source can also be interpreted as meaningful societal outcome is not so easy to show, but might be a next useful logical research step.

The conundrum for open source exploitation is that it transcends the intelligence community. It provides a window onto reality for anyone. The challenge is not whether the intelligence community are the preferred supplier of truth to power but whether power is getting the best truth and also capable of making the best judgements. It does not really matter how efficient the exploitation of open source is or becomes if policy is shaped in the absence of best truth.

References and Notes:

[1] US Commission on the Roles and Capabilities of the United States Intelligence Community (Aspin-Brown Commission), 1996, *Preparing for the 21st Century: An Appraisal of US Intelligence*, Washington, DC: US Government Printing Office, p.xxi.

[2] Croom, H.L., 1969, 'The Exploitation of Foreign Open Sources', *Studies in Intelligence*, 13, 2 (Summer), pp.129-136. NB. This is a declassified secret document and 2 versions of it exist, see: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB90/index.htm documents 7A & 7B

[3] The BBC Monitoring Service is now known simply as BBC Monitoring. For a more comprehensive history of BBC Monitoring's establishment, see: Renier, O., Rubinstein, V., 1986, *Assigned to Listen: The Evesham Experience 1939-1943*, London: BBC Books, pp.9-23.

[4] Similarly, for a concise history of the emergence of FBIS, its name changes, its 'scoops' and literally its trials and tribulations, see: Mercado, S.C., 2001, 'Open Source Intelligence from the Airwaves: FBIS Against the Axis', 1941-1945, *Studies in Intelligence*, Fall-Winter, 11, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/fall_winter_2001/article04.html

[5] Renier & Rubinstein note that the Foreign Office had been monitoring similar broadcast some months earlier, see: Renier, O., Rubinstein, V., 1986, *op cit*, pp.13-14.

[6] Herman, M., McDonald, J., Masny, V., 2006, *Did Intelligence Matter in the Cold War?* Oslo: Institutt for Forsvarsstudier (Norwegian Institute for Defence Studies).

[7] RAND National Security Research Division & Office of DNI, 2006, *Towards a Theory of Intelligence*, Washington: RAND, p.7.

[8] Held, D., 2004, *Global Covenant*, London: Polity Press.

[9] The 'threat-list' varies. These are collated from: US Office of the Director of National Intelligence, Annex to the US National Intelligence Strategy, 2006, *The US Intelligence Community's Five Year Strategic Human Capital Plan*, US DNI, Washington, and: US National Intelligence Council, 2004, *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project*, US National Intelligence Council, Washington, available at: http://www.foia.cia.gov/2020/2020.pdf

[10] http://www.aim25.ac.uk/cgi-bin/search2?coll_id=1580&inst_id=13. Interestingly, one of its production lines was the creation of working maps.

[11] Google's company-overview, line one, available at: http://www.google.com/corporate/

[12] Steele, R.D., 2001, *On Intelligence: Spies and Secrecy in an Open World*, Oakton, Virginia: OSS International Press, p.xi.

[13] In Ackerman, R., 2006, 'Intelligence Center Mines Open Sources', *SIGNAL Magazine*, March 2006, available at: http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1102&zoneid=31

[14] For an extraordinary example of 'mashing-up', which also raises issues of privacy, regulation as much as open source potential, see: http://www.georgia-sex-offenders.com/maps/offenders.php ; See: http://www.usnews.com/usnews/news/articles/061029/6outreach.htm and particularly http://www.nytimes.com/2006/12/03/magazine/03intelligence.html?ex=1322802000&en=46027e63d79046ce&ei=5090&partner=rssuserland&emc=rss for the DNI's creation of wiki-based analysis designed to encourage information sharing.

[15] See: US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company, p.413; Silberman, L., Robb, C., 2005, *US Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC: Report No: 20503, pp.377-380.

[16] In particular, see Dearlove & Quiggin for a brief summary of how the clandestine side of intelligence is changing as a result of ephemeral new terrorism at: http://www.isn.ethz.ch/news/sw/details.cfm?ID=16521; US Intelligence Reform and Terrorism Prevention Act, 2004; US Presidential Executive Order, No: 133888, 2005, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, available at: http://www.fas.org/irp/offdocs/eo/eo-13388.htm ; US Attorney General, 2003, *Memorandum of Understanding Between Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing*, dated: 4 March 2003, available at: http://www.fas.org/sgp/othergov/mou-infoshare.pdf ; Thompson, B.G., 2006, *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*, Washington: US House Committee on Homeland Security Democratic Staff; RAND National Security Research Division & Office of DNI, 2006, *op cit*, p.1.

[17] In initial contacts with GCHQ and HMRC, it was made explicit to the author that part of the reason that engagement with this research could not be entered into was precisely because they were unable to separate out their closed and open activities. See Chapter Four (4.2.5).

[18] This has been made explicit in the UK by the appointment of a Professional Head of Intelligence Analysis within the Cabinet Office with responsibility for analysis across the intelligence community.

[19] Keegan, J., 2003, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, (Pimlico Edition 2004), London: Pimlico, p.20.

[20] Gibson, S., 2005, 'In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation', *Risk Management: An International Journal*, 7, 4, pp.23-41.

[21] Warner, M., 2002, 'Wanted: A Definition of Intelligence', *Studies in Intelligence*, 46, 3, available at: http://www.au.af.mil/au/awc/awcgate/cia/define_intel.htm

[22] RAND National Security Research Division & Office of DNI, 2006, *op cit*, p.2.

[23] Berkowitz, B., Goodman, A., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press, pp.58-98; RAND National Security Research Division & Office of DNI, 2006, *op cit*, pp.21-22.

[24] Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

[25] RAND National Security Research Division & Office of DNI, 2006, *op cit*.

[26] US Senate Committee on Armed Services, Hearings on the National Defense Establishment, 1st Session, 1947, pp.525-528, as recounted in Peter Grose, 1994, *Gentleman Spy: The Life of Allen Dulles*, New York: Houghton Mifflin, p.275.

[27] Conversations with Michael Herman (former secretary to the UK Joint Intelligence Committee) and Dr Joe Markowitz (former Director of the US government's (CIA) Community Open Source Programme) and endorsed by the UK's Open Source Joint Working Group.

[28] Conversation with Dr Joe Markowitz former Director of the US government's (CIA) Community Open Source Programme.

[29] See for example: Steele, R.D., 2004, 'Accessing the Full Range of Open Sources', *International Journal of Intelligence and CounterIntelligence*, 17, 1, p.183, where he asserts that: "The reality is that during the Cold War the US exploited, at best, perhaps 20 percent of the available open sources."

[30] Odom, W., 2003, *Fixing Intelligence for a more Secure America*, New Haven: Yale, p.32; RAND National Security Research Division & Office of DNI, 2006, *op cit*, pp.26-29; Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press, p.18.

[31] For an expression of the relationship between truth, reality, and trust see: David Young, Reuters Fellows Lecture, *Scholarship, Intelligence and Journalism*, 10 March 2004, in Oxford Analytica, 2006, (Ed) *Spies, Lies & Intelligence: A Briefing Book prepared by Oxford Analytica*, Oxford: Oxford Analytica.

[32] Florini, A., 2003, *The Coming Democracy: New Rules for Running a New World Order*, Washington: Island Press.

[33] Rolington, A., 2006, 'Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11', *Intelligence and National Security*, 21, 5, pp.741-742.

[34] See for example: Council of the European Union, (Ed) 2005, *The European Union Counter-Terrorism Strategy*, Brussels: Council of the European Union, Report No: 14469/4/05 REV 4, pp.13-14, where they explicitly request such cooperation and exchange within and between organisations such as EUROPOL; Eurojust; and the Situation Centre.

[35] Search using "sharing" at http://www.fas.org/blog/secrecy, and as one example: http://www.fas.org/sgp/news/secrecy/2005/04/040805.html#2

[36] Betts, R.K., 1978, 'Analysis, War, and Decision: Why Intelligence Failures are Inevitable', *World Politics*, 31, 1, pp.61-89.

[37] Hillson, D., Murray-Webster, R., 2005, *Understanding and Managing Risk Attitude*, Aldershot: Gower Publishing.

[38] Taleb, N.N., 2007, *The Black Swan: The Impact of the Highly Improbable*, London: Penguin.

[39] In both the US and UK 'champions' of open source exploitation have been established. In the UK the Open Source Joint Working Group was established in 2000. An International Open Source Working Group covering 12 countries was established in 1995.

[40] In the US, the creation of the Open Source Center was approved by the DNI on 8 November 2005: https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2005/pr11082005.html Some are exerting pressure to create an open source agency *external* to any government control.

[41] Perl, R., 2005, *Combating Terrorism: The Challenge of Measuring Effectiveness*, Washington: Congressional Research Service: The Library of Congress, Report No: RL33160, p.1.

[42] *Ibid*, p.2.

[43] Bull, 2005, as discussed in: Hillson, D., Murray-Webster, R., 2005, *op cit*, p.11.

[44] See the UK's *National Intelligence Machinery* booklet, p.6, available at: http://www.intelligence.gov.uk/publications/documents/national_intelligence_booklet.pdf

[45] A question presented to the author by an analyst on the Cabinet Office Analysts Course.

[46] http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=1102&zoneid=31

[47] McGee, A., 2007, *Corporate Security's Professional Project: An Examination of the Modern Condition of Corporate Security Management and the Potential for Further Professionalisation of the Occupation*, Department of Defence Management and Security Analysis, Cranfield University.

[48] Full access to this website resource is only available to members of the US Intelligence community and US Library of Congress. They have access to search the databases of ten commercial providers: *Economist Intelligence Unit; ProQuest Databases; Oxford Analytica; Strategic Forecasting (Stratfor); EbscoHost Research Databases; Janes; NewspaperDirect; IEEE Xplore Database; Business Monitor International.* Interestingly, and by comparison, Cranfield University subscribes to some 69 databases at the time of writing including seven on this list or their equivalents.

[49] Giles, L., 1910, *Sun Tzu: The Art of War*, translated from the Chinese and now available at: http://www.yuni.com/library/suntzu.htm (13:2)

[50] *Ibid*, (13:3)

[51] See note 92 of Chapter Two

[52] National Intelligence Machinery Booklet available at http://www.intelligence.gov.uk/downloads/index.asp p.6.

[53] Ackerman, R.K., 2006, *op cit.*

[54] The novel *Pamela: Or, Virtue Rewarded* by Samuel Richardson and published in 1740 was considered at the time to herald the downfall of the young simply because it meant that young people developing a

fascination for these new 'racy' novels would waste their time by reading them; much the same is considered of *Game Boy* today, for example.

[55] Rogerson, S., 2007, *'The Ethical Challenge of Information Provision'*, paper delivered at Cranfield University, Shrivenham, 15 May 2007, in which he made the comment and repeated it twice further to ensure effect.

[56] Ackerman, R.K., 2006, *op cit.*

[57] Borodzicz, E., 2005, *Risk, Crisis and Security Management*, Chichester: John Wiley & Sons.

[58] Sunstein, C.R., 2005, *Laws of Fear: Beyond the Precautionary Principle*, Cambridge: Cambridge University Press, pp. 109-128.

[59] See: Surowiecki, J., 2004, *The Wisdom of Crowds*, London: Little Brown; Rheingold, H., 2002, *Smart Mobs: The Next Social Revolution*, Cambridge, MA: Basic Books; Reynolds, G., 2006, *An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government and Other Goliaths*, Nashville, TE: Nelson Current; Levine, R., Locke, C., Searls, Doc., Weinberger, D., 2000, *The Cluetrain Manifesto: The End of Business as Usual*, Cambridge, MA: Perseus Books Group; McMurray, J., 2006, 'Social Search Promises Better Intelligence', Associated Press, 9 July 2006, available at: http://msnbc.msn.com/id/13740161/

[60] See: McMurray, J., 2006, *op cit.*

[61] W.H. Smith Limited, 1992, *Shakespeare: The Complete Works*, Bath: The Bath Press, p.400.

[62] For a useful analysis of war in these dimensions see: Gray, C.S., 2005, *Another Bloody Century: Future Warfare*, London: Weidenfeld & Nicholson.

[63] Keegan, J., 2003, *op cit*, p.21.

[64] Aldrich, R.J., 2005, 'Setting Priorities in a World of Changing Threats', *NATO Workshop on Intelligence Reform*: St Anthony's College, Oxford.

[65] In the 2006 US National Intelligence Strategy, terrorism tops the list of strategic threats, while globalisation is at number four. See: US Office of the Director of National Intelligence, *The US Intelligence Community's Five Year Strategic Human Capital Plan*, (Washington: US DNI 2006), Annex to the US National Intelligence Strategy, pp.3-4.

[66] Steele, R.D., 2006, in *Strategic Intelligence Ed Loch Johnson*, available at: http://www.oss.net/dynamaster/file_archive/060409/00b583e458c7fb78e96ddc3a8444ae30/STEELE%20Draft%20Chapter%20for%20Strategic%20Intelligence%20on%20OSINT%2c%202.4.doc p.16.

[67] This notion is supported by remarks made at St Anthony's College, Oxford on 7 March 2006 by Professor Ray Halliday at the Leverhulme Parliamentary Fellows seminar and in RAND National Security Research Division & Office of DNI, 2006, *op cit*, p.26.

[68] For a treatment of the importance of denominators in contemporary risk society see: Tallis, R., 2004, *Hippocratic Oaths: Medicine and its Discontents*, London: Atlantic Books, pp.166-174.

[69] See: Herman, M., McDonald, J., Masny, V., 2006, *op cit*; Rolington, A., 2006, *op cit*.

[70] See: http://www.cognitive-edge.com/presentationdetails.php?presentationid=3

[71] Hillson, D., Murray-Webster, R., 2005, *op cit*.

[72] Hunt, B., 2004, *The Timid Corporation: Why Business is terrified of Taking Risk*, London: Wiley, pp.83-102.

[73] Power, M., 2004, *The Risk Management of Everything*, London: Demos.

[74] Barnett, R., 1990, *The Idea of Higher Education*, Buckingham: Open University Press.

[75] Tallis, R., 2004, *Hippocratic Oaths: Medicine and its Discontents*, London: Atlantic Books.

[76] Power, M., *op cit*; Hunt, B., *op cit*.

[77] Saatchi, M., (Ed) 2006, *In Praise of Ideology*, London: Centre for Policy Studies.

[78] For the 'risk society' thesis see: Beck, U., 1992, *Risk Society: Towards a New Modernity*, London: Sage Publications; Giddens, A., 2002, *Runaway World: How Globalisation is Reshaping Our Lives*, London: Profile Books; Rischard, J.F., 2002, *High Noon: 20 Global Issues, 20 Years to Solve Them*, Oxford: Perseus Press; Rees, M., 2003, *Our Final Century: Will the Human Race Survive the Twenty-First Century*, London: William Heinemann.

[79] For the anti 'risk society' thesis see: Mythen, G., 2004, *Ulrich Beck: A Critical Introduction to the Risk Society*, London: Pluto Press; Feldman, S., Marks V., 2005, *Panic Nation: Unpicking the Myths We're Told About Food and Health*, London: John Blake Publishing Ltd.; Bate, R., 1999, *What Risk?: Science, Politics & Public Health*, Oxford: Butterworth-Heinemann. ISBN: 0-7506-4228-9; Lomborg, B., 2001, *The Skeptical Environmentalist: Measuring the Real State of the World*, Cambridge: Cambridge University Press; Burgess, A., 2004, *Cellular Phones, Public Fears, and a Culture of Precaution*, Cambridge: Cambridge University Press.

[80] Popper, K.R., 1945, *The Open Society and its Enemies - Volume One: The Spell of Plato*, Routledge & Keegan Paul, 2nd Ed & Reprint 2005, pp.35-55.

[81] Better Regulation Commission, 2006, *Risk, Responsibility and Regulation: Whose Risk is it Anyway*, London: Better Regulation Commission, available at: http://www.brc.gov.uk/publications/risk_report.asp

[82] Sunstein, C.R., 2005, *op cit*.

[83] For example see: http://www.sciencenews.org/articles/20030111/fob3.asp

[84] McInnes, C., 'Health, 2005, Security and the Risk Society', *Nuffield Trust Paper - Health, Security and Foreign Policy Programme*, available at: http://www.nuffieldtrust.org.uk/publications/detail.asp?id=0&PRid=200

[85] Durodie, W., 2005, *The Domestic Management of Terrorist Attacks*, Report No: L147251003, London, available at: http://www.terrorismresearch.net

[86] Walsh, B., 2006, 'The Deadly Side Effect of Avian Flu', *Time*, 27 February 2006.

[87] O'Neill, O., 2002, *A Question of Trust: The BBC Reith Lectures 2002*, Cambridge: Cambridge University Press, pp.15-19.

[88] Silberman, L., Robb, C., 2005, *US Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC: Report No: 20503, pp.13,36,147, and 560.

[89] Better Regulation Commission, 2006, *op cit*, p.45.

[90] *Ibid*, pp.40-41.

[91] The Butler Review noted that SIS was working with up to five sources of varying reliability. See: UK Privy Councellors, (Ed) 2004, *Review of Intelligence on Weapons of Mass Destruction (The Butler Review)*, House of Commons, HC 898, pp.74 and 100-102.

[92] Aldrich, R.J., 2005, *op cit*.

[93] Remark made during a presentation under Chatham House rules at St Anthony's College, Oxford, 2007.

[94] Rischard, J.F., 2002, *op cit*; US National Intelligence Council, (Ed) 2000, *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, US National Foreign Intelligence Board under direction of the DCI, NIC 2000-02; US National Intelligence Council, (Ed) 2004, *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project*, Washington: US National Intelligence Council.

[95] Gray, C.S., 2005, *op cit*; Runciman, D., 2006, *The Politics of Good Intentions: History, Fear and Hypocrisy in the New World Order*, Woodstock: Princeton University Press.

[96] James, O., 2007, *Affluenza*, London: Vermilion.

[97] Slovic, P., 2000, *The Perception of Risk*, London: Earthscan.

[98] For a science-based treatment of some contemporary myths see: Feldman, S., Marks Vincent., 2005, *Panic Nation: Unpicking the Myths We're Told About Food and Health*, London: John Blake Publishing Ltd.

[99] Gill, P., Phythian, M., 2006, *op cit*, p.172.

[100] Rischard, J.F., 2002, *op cit*.

[101] Popper, K.R., 1945, *op cit*, p.xix.

[102] Manunta, G., 1998, *Security: An Introduction*, Cranfield University.

[103] Sunstein, C.R., 2005, *op cit.*

[104] Aldrich has used the more expressive term: "refuse collectors of globalisation".

[105] See: Ross, C., 2007, 'In the Matrix, You Mess up Foreign Policy', *The Sunday Times*, 18 February 2007, News Review, p.4.

[106] Gill, P., Phythian, M., 2006, *op cit*, p.1.

[107] Furedi, F., 2005, *Politics of Fear*, London: Continuum.

[108] For a timely and relevant example of this paradox, see: Mirza, M., Senthilkumaran, A., Ja'far, Z., (Eds), 2007, *Living Apart Together: British Muslims and the Paradox of Multiculturalism*, London: Policy Exchange, Report No: 241, available at: http://www.policyexchange.org.uk/images/libimages/241.pdf

[109] Devji, F., 2005, *Landscapes of the Jihad: Militancy, Morality, Modernity*, London: C. Hurst & Co.

[110] *Ibid*.

[111] Gray, C.S., 2005, *op cit*.

[112] Blair, T., 2006, *A Global Alliance for Global Values*, (London: Foreign Policy Centre 2006).

[113] Saatchi, M., 2006, *In Praise of Ideology*, London: Centre for Policy Studies.

[114] Gray, C.S., 2005, *op cit*.

[115] At the time of completion of this thesis, a set of attempted bombings had just taken place in London and Glasgow in June2007. It is too early to tell whether they are politically or quasi-nihilistically inspired, but they were certainly shambolic.

[116] Friedman, T.L., 2006, *The World is Flat: The Globalized World in the Twenty-First Century*, London: Penguin Books.

[117] See: Ross, C., 2007, *op cit.*

[118] Berkowitz, B.D., Goodman, A.E., 2000, *op cit*; Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press.

[119] Warner, M., 2002, *op cit*; Warner, M., 2006, 'The Divine Skein: Sun Tzu on Intelligence', *Intelligence and National Security*, 21, 4, pp.483-492.

[120] A similar conclusion is drawn by Gill and Phythian, see: Gill, P., Phythian, M., 2006, *op cit,* pp.1-19.

[121] *Ibid*, pp.29-38.

[122] On the other hand how can you have a theory of intelligence when, like politics itself, it is so much more about the interaction of personalities with power than power's interaction with the abstracts it constructs – intelligence or politics.

[123] Rawnsley, A., 2001, *Servants of the People: The Inside Story of New Labour*, London: Penguin Books.

[124] Hood, C., Heald, D., 2006, *Transparency: The Key to Better Governance?*, Oxford: Oxford University Press, ISBN: 978-0-19-726383-9.

[125] See: US Congressional Research Service, 2006, *9/11 Commission Recommendations: Implementation Status*, Washington: Congressional Research Service, Report No: RL33742, available at: http://www.fas.org/sgp/crs/homesec/RL33742.pdf.

[126] Power, M., 2004, *op cit*.

[127] O'Neill, O., 2002, *op cit*, p.70; O'Neil, O., 2006, 'Transparency and the Ethics of Communication', in Hood, C., Heald, D., 2006, *op cit,* pp.75-90.

[128] O'Neill, O., 2002, *op cit*, p.70.

[129] OSS CEO: 'Comments on Exxon Mis-Information (Or Active Lies) to the Public With Respect to Peak Oil - Culprits Should be Fired - Collective Intelligence (Legal Ethical Open Source Intelligence or OSINT) in the Public Interest' at: http://www.oss.net/extra/news/?module_instance=1&id=2498 dated 2 March 2006

[130] See the recent UK report on regulation: Better Regulation Commission, 2006, *op cit.*

[131] As quoted in: Popper, K.R., 1945, *op cit*, p.xx.

[132] Betts, R.K., 1978, *op cit*.

[133] Barger, D., (Ed) 2005, *Toward Revolution in Intelligence Affairs*, Arlington, VA: RAND.

[134] Interestingly, one might attribute the 'failure' of OSINT to 'catch-on' more to structural and cultural issues than to anything peculiar to OSINT. The current demise of EUROPOL's OSINT effort can be placed at the cultural even personal door. The DIS struggles on both counts. It is structurally challenged in that the MOD is a hugely disparate organisation being physically located all over the globe and has a corporate body in the hundreds ***of*** thousands rather than hundreds ***or*** thousands. It is culturally challenged in that it has not passed the boardroom test of selling itself in terms of customer efficacy, which are variously contractual, personal and, in the UK MoD, locational.

CHAPTER SIX

CONCLUSION

> "Much of the study of intelligence concerns the relationship between power and knowledge, or rather the relationship between certain kinds of power and certain kinds of knowledge."
>
> Scott & Jackson, 2004[1]

6.0 Introduction

The research question set the working hypothesis that open source exploitation contributes to intelligence in a way that can be described by a set of key high order factors. The data and analysis show that such factors do exist and are strongly articulated by intelligence practitioners. Indeed, the set of factors form a useful model that seems generalisable. The supporting research objectives are also achieved: notably the identification and plugging of a gap associated with the understanding of open source exploitation; and recommendations for policy concerning open source exploitation.

Undoubtedly, and ironically, the broader and more public examination of intelligence as a result of the plethora of inquiries post-9/11, and subsequently the question of WMD in Iraq, made access to the intelligence community more likely than had they not happened. 9/11 and Iraq, in western societies, have together precipitated an explosion of interest in the intelligence function of government. Its relationship with politics, including its very idea and purpose, are now commonplace questions for official and unofficial scrutiny.

Nevertheless, the genesis of this research remains rooted in the fundamental transformation in ICT that has occurred over the last two decades. Set against that background, 9/11 and Iraq were merely catalysts that sped the growing significance of open source exploitation, already and inevitably underway. Only seven years ago, when the research idea was conceived, the exploitation of open sources of information was largely confined to public sector organisations exploiting information sources residing in the public domain - Reuters, Factiva, Janes, Experian, *The Economist* amongst many others - something that librarians,

inside and outside intelligence communities, had been doing for some time. Now, the number of sources, access routes to those sources, and methods by which to analyse the information from those sources, have all expanded considerably. In short, a once cottage-based exploitation has begun to industrialise across all sectors, within many societies, and for many purposes. The same is true for intelligence communities, although their experience of this transformation has been a varied one.

To the quote at the start of this chapter, Gill and Phythian added: "Arguably all the non-trivial study of intelligence is concerned with this relationship."[2] Conforming to this, as well as their exhortation of interplay between theorising and empiricism, this thesis has conducted empirical research into the operational significance of open source exploitation and derived empirically the unique contribution that open source exploitation makes to the intelligence function in the form of high order factors. It has then attempted theoretical abstraction by answering the question - so what - with regard to the interplay between knowledge and power.

6.1 Overview

Chapter One set the scene and the context for the study. On the one hand, there is recognition of a qualitative and quantitative change in open source potential courtesy, largely, of the contemporary transformation in ICT. On the other hand, deeper global influences - globalisation, risk society, and changing societal expectation - are changing the contemporary environment that intelligence is trying to understand. Yet, western polities, at least, have merely been persuaded to realign their security focus from a post Cold War 'drift' to the threat of 'new terrorism'.

Chapter Two identified the research gap. There was no description of a common understanding of the contribution of open source exploitation to the intelligence function in the literature: implicitly because there is a simple lack of it; and explicitly because what is

said is discordant. Certainly, the literature specific to open source intelligence is rare by comparison to the more traditional closed intelligence function. It is mentioned more in passing than treated as a subject in its own right. The practitioner literature is dominated by a single source: US-oriented; strident in tone; and often antagonistic to the closed intelligence community. The academic literature comprises no more than a handful of efforts to explain why open source exploitation might be useful, but it is minimal, inconsistent, and explicitly unsupported. This research effort provides a considerable body of demonstrable, coherent, and new evidence to explain the open source contribution.

Chapter Three structured the research methodology. It emphasised the case-study approach as basis for the research method, participant observation and semi-structured interview for extracting data, and the use of comparative analysis in order to generate a theory in the form of a model. The very responses to requests for access tell their own separate story about the internally perceived benefits of open source exploitation, as well as an externally imposed need for intelligence to adjust to bigger contemporary geo-political and socio-cultural influences through 'outreach'. Approaches to engage with HMRC and GCHQ as in-depth case-studies were rejected in March 2005. DIS, although content to engage with the research at the level of the OSINT cell were unable to expand the engagement into a more formal in-depth case-study. However, in November 2005, the author was invited to engage with the UK intelligence community's Open Source Joint Working Group (OSJWG) on which both GCHQ and DIS are represented and much of the UK intelligence community's open source exploitation effort is coordinated and developed.

Chapter Four essentially built, developed, and tested a model of high order factors that describe the open source contribution to the intelligence function. These factors are named as: context; utility; focus; cross-check; surge; communicability; and analysis. They were successfully tested against an in-depth case-study - the Asian Studies Detachment.

Chapter Five analysed the results and discussed the implications for open source exploitation at an operational level, including open source organisation, location,

capabilities, principles, barriers, and issues for policy and doctrine. However, it is difficult not to relate the emergence of open source and its relationship with intelligence to the broader contextual issues influencing contemporary society. Thus, Chapter Five also discussed this reflexive arrangement, whereby the drivers that shape the geo-political and socio-cultural context that intelligence is trying to understand also simultaneously shape its own conduct.

6.2 The same changing story

The fortunes of open source exploitation have been mixed. During the research period, both the UK and US have established new open source champions; the US has established a dedicated national Open Source Center and the UK's JIC unusually discussed the significance of open source exploitation as a discrete subject in its own right. Meanwhile, two of the preliminary research case-studies - EUROPOL and VIC/APAN - have closed down their open source efforts. Yet, many other open source efforts have emerged in many private sector enterprises, and notably within the US and UK military, as 'extra' to pre-existing closed intelligence efforts or 'expeditionary' to new areas of operation.

Two further phenomena coincided with and reinforced this nascent exploitation of open source during the research period. First, the quietly emerging private security sector of post-1989 second-career soldiers and policemen was rocketed to prominence by 9/11 at 'home', and Iraq, principally, abroad. This included the production of intelligence by and for its own sector via a third wave of 'migrant' workers to the sector from the public sector intelligence community. While the explosion of private sector intelligence may represent a competitor to the traditional public sector monopoly, their purpose and interests remain unitary and broadly aligned towards safeguarding economic prosperity, the delivery of security, and a commonly held view of foreign policy interests. Second, and more recently, the open source domain has itself expanded as a result of further developments, innovations, and applications of ICT. This is most graphically encapsulated by terms such

as ‘user-generated content’, ‘new social media’ and ‘social networks’. They represent a significant emergent issue for traditional intelligence in terms of telling truth to power. Not because they are necessarily capable of better representing reality, but because they create multiple versions of reality with increasingly diverse and numerous purposes and interests that presently defy arriving at a rational or common universality.

So, not only is intelligence, like security, going ‘private’, but it is also becoming, so-called, ‘democratised’. The former may be mildly aggravating to the traditional public sector intelligence and security community. However, their broadly common goals, if not personal former establishment relationships, maintain a broadly common direction. The latter is fundamentally more troublesome; perhaps for the conduct of politics more so than intelligence. The line between an optimistic transforming digital democracy and a hopeless self-absorbed useless ‘digital solipsism’ seems very fine indeed. Then again, it is early days, and perhaps no more than the contemporary manifestation of all previous forms of mediated hyperbole. But, like its enabler, the contemporary transformation in ICT has conferred both an industrial and immediate scale unseen before.

More optimistically, there is very little genuinely new under the sun. Much of what appears new is simply that: perceived new to us. The same is true of our treatment of information. At least three constant guiding principles should be remembered. First, that information, whether openly or clandestinely acquired remains subject to some simple but universal rules of information-working: validity; reliability; accuracy; and timeliness. Second, the information market is imperfect. In particular, it remains the case today that human beings, with their attendant biases and frailties, still have to interpret it by way of analysis and assessment. Third, notwithstanding the challenges of ensuring the integrity of the analytical process, there remains a continued need to debate and win arguments utilising its assessment. In the face of so many perceived versions of reality, this has never been more urgent for policy-makers. In all these regards, the role of intelligence as principal providers of truth to power is similarly challenged.

6.3 Beyond operational: The contextual contribution of open source exploitation

Open source exploitation is a somewhat schizophrenic phenomenon. It has very practical application to the conduct of intelligence at the operational level, which is where this work started. Understanding that contribution in the form of a model of high order factors is a useful start point from which one might begin to determine how best to harness it for purposeful ends. However, the transformation in ICT and the attendant transformation in open source exploitation transcend the merely operational. They are shapers of context as well as tools for understanding context. This thesis identified and examined three significant drivers of context: globalisation; risk society; and changing societal expectations. They are all deeply influenced by the recent transformation in ICT, forming both virtuous and vicious feedback loops into the construct of context. Globalisation is probably the most widely recognised, risk society the most pernicious, and changing expectations the least understood. They all represent a challenge to intelligence in terms of understanding, as well as informing, the relationship between knowledge and power. Thus, it has been inescapable to analyse the subject of open source on anything less than two levels: the operational and the contextual.

An important part of the contextual aspect, particularly changing expectations, is the contribution of the transformation in ICT to openness in the sense of transparency. It has become a perceived vital ingredient of good governance and shaper of intelligence conduct from the outset. The more intriguing and perhaps more valuable contribution for further research may prove to be the deeper implications of this so-called openness for the conduct of intelligence and the context in which intelligence is conducted.

Yet, the transformation in ICT also contributes to the social, cultural and political context, which intelligence is charged to fathom. At the very least, it raises questions for contemporary society as to where the conduct of intelligence resides, the definition of intelligence as classically understood, and the purpose of intelligence in terms of the real targets for intelligence activity. It is unsurprising that some of the most recent academic

literature on intelligence is attempting to grapple with these questions through the formulation of a 'theory of intelligence' that characterises, at its heart, the relationship between power and knowledge.

The author has suggested that this 'problem' may very well be no more than 'new wine in old bottles': that any theory of intelligence might usefully start from the assumption that the nature of intelligence does not change while its character evolves relentlessly; that intelligence by definition is no more or no less than support to decision making; that intelligence is nothing more special than a sub-set of information or decision theory.

6.4 Key findings

The key findings pertinent to open source exploitation across the thesis are:

- Open source information is formally exploited for intelligence purposes in security, law enforcement, and defence organisations commonly found in a national public sector. Comparable multi-national, regional, and inter-governmental organisations do so too. Similarly, private, NGO, and academic sector organisations do so as the only option in the absence of closed information.
- Open source exploitation is not undertaken uniformly across these organisations in terms of 'best practice', in terms of resource, or in terms of meaningful outcome. Yet, however haphazardly, open source doctrine, policy and training are being established within intelligence communities. This leadership is represented by organisations such as the US National Open Source Enterprise under the leadership of the AD/DNI-OS and the Open Source Center, as well as the UK's Open Source Joint Working Group comprising representatives of the Single Intelligence Account and associated organisations. Less formal arrangements also occur where coalition or intergovernmental activity necessitate collaboration, such as CENTCOM for the conduct of coalition operations in Iraq and Afghanistan.

- The contemporary exploitation of open source information does not represent a revolution in intelligence affairs. The nature of intelligence - support to decision-making - remains extant. Open source exploitation might more accurately be portrayed as a consequence, albeit a significant consequence, of the contemporary transformation in ICT, which the intelligence community would, of necessity, be interested in. They are and have been.
- The contemporary exploitation of open source information does represent a change in the character or conduct of the intelligence function. This is reflected with varying degrees of success and methodology at the operational level. The key high order factors, detailed in Chapter Four - context, utility, focus, cross-check, surge, communicability, and analysis - describe the contribution of open source exploitation to the intelligence function as a whole. Although, they are not all equally and similarly pursued.
- Open source exploitation remains a poor relation of the traditional closed intelligence disciplines. It is certainly relatively under-resourced. It is absolutely under-resourced if its contribution to output is a defensible determinant. Culturally, it still attracts an institutional snobbery prejudiced against it in favour of closed. This snobbery is itself curious. The most senior practitioners of intelligence abhor such a prejudice. Many individuals within the agencies visited in this research decry it. Yet, institutionally, there remains a cultural proclivity towards it. More intriguingly, this apparent discrepancy between personal and institutional viewpoints on this issue can be seen to be carried by a single individual at the same time. Because open source exploitation is essentially perceived not 'secret', it carries a cachet that associates it with being 'cheap' and 'easy'. More worrying intellectually is the acculturated association and equating of open source with unreliability; often erroneously stated as: "if it's (sic) on the Internet then it must be rubbish". Like most prejudice, it derives in part from ignorance, in part from resistance to change, and partly, because of its specific genesis in the contemporary digital version of ICT transformation, to a generational techno-phobia. However, ignorance must also be attributed in some degree to open source practitioners' own failure to convincingly demonstrate effectiveness.

- In most organisations, operating in the real world of limited resources, new functions tend to establish themselves, in terms of effectiveness, at the expense of the established. Yet, other than SOCOM, open source contribution is rarely seen being 'measured' deliberately against closed intelligence. The case-studies more closely reflect the approach of ASD, where practitioners go out of their way to articulate the collaborative nature of open and closed. By contrast, articulating efficiency, at the outset at least, seems a reasonable and well-trodden course of action by all the case-studies. It seems a vital first step for open source efforts that intend to stay the course; the more successful ones tending to maintain it. Indeed, all the cases studies demonstrate their efficiency as a resource for the collective good. However, at some point the critical relationship between resource allocation and objectives - efficacy - has to be addressed holistically, and for open source this seems sensible within the intelligence system and only by way of comparison to closed.
- It is not sufficient to merely establish an open source effort in order to deliver the contributing factors. Good old-fashioned internal structural and cultural barriers (office politics) play as much a part in failure as the demonstration of efficacy does to success. This is most accurately shown by the demise or thriving of open source efforts within intelligence agencies. At the time of submission of this thesis, the EUROPOL open source cell has been wound-up, the VIC/APAN cell has been transferred to the Personnel Branch, and the DIS effort remains unclear as it returned to 'in-house' status from the outsourced contractor arrangement with effect October 2006. By contrast, the agencies within the UK's SIA have strengthened budgets and resource, the ASD has assumed responsibility for open source where VIC/APAN has been withdrawn, SOCOM demonstrably thrives on its open source initiative, and the DIA have appointed Mr James G. Noone to be its first Open Source Program Office Chief. Thus, personalities and politics are as instrumental in defining pathways to success as the subject matter itself, whatever the organisation. OSINT is no exception.
- The more successful organisational model for the process of open source exploitation is nearer to a decentralised 'push' than a centralised 'pull' structure. That is to say open source exploitation is deemed most effective when made available at the customer point

of production rather than when retrieved by the customer from the point of collection. In some public sector organisations a hybrid system operates, whereby open source specialists are both deployed 'outwards' as well as retained 'centrally'. That is to say open source specialists are situated alongside analysts rather than geographically dislocated from them, while a core of expertise is 'held in reserve' for more difficult requirements. While the research indicates that this is perceived to be the optimal structure; resource constraints often prevent optimisation.

Two related and debateable issues emanate from this preferred process. First, the combination of analysis with open source exploitation in one person (the analyst) is not necessarily the obvious corollary. Where public sector open source efforts require that analysts do their own open source exploitation, as well as closed analysis, it logically follows that, if a surfeit of closed information is already overloading capacity, then adding open source exploitation would only prove more detrimental. The assumption that open source exploitation is simply attending to the Internet obfuscates the time, skill, and experience necessary to 'search smart', as well as misses the fundamental breadth of open sources beyond the Internet. Conversely, in private sector information brokerages, at the outset at least, the analyst and open source specialist is more often one and the same person. This partly reflects the operational and resource constraints experienced 'along the way' in creating capacity and capability, rather than any deliberate policy at the outset. Partly, it also reflects the locus of genuine expertise. However, eventually, such organisations are forced to separate out the collection and analysis effort in line with escalating demand and scale. Second, the clinical division of collection and analysis, represented perhaps by the establishment of a separate open source 'agency' dedicated to open source exploitation, is similarly *non sequitur*. In the US, largely because of the economies of scale, open source exploitation has been constructed in significant discrete chunks giving the appearance of a distinct discipline rather than a separate agency. Yet, the contribution of open sources to intelligence is now recognised as being so inextricably entwined with each intelligence discipline, at all stages of the intelligence cycle, that separating it out may prove more damaging than

the undoubted benefits of operating outside the security constraints of a closed environment. It may be that both extremes are possible where resource and commitment dictate. However, even if both extremes were implemented, it is unlikely that it would be at the expense of the notion of distributed, enmeshed, dispersed open source exploitation.

- Internal efficiency is no substitute for external effectiveness. The research confirms the popular notion that, for certain intelligence targets, the contribution to final intelligence product of open source relative to closed is adjudged 'high'. The 80 percent rule has become the rule of thumb. Yet, nowhere is it explicitly stated how it is derived or measured. More importantly, it does not convey 'why' or 'how'. Thus, while it may actually be so, the rule is at worst misleading or at best irrelevant. There are many competing and reasonable explanations for the predominance of open source: there is more of it; it is easier to handle; it is more readily available; it has always been that way. Internally, and by comparison to closed, it can be shown to be effective; but when viewed from outside, a more discerning test of meaningful outcome should be applied: exactly where and how does it contribute? It is hard enough to debate the notions of intelligence success and failure without having to apportion blame to a particular intelligence discipline. Organisational success and failure is not peculiar to the intelligence community. Again, the usual cultural suspects are more prominent than the technical.
- Like much of contemporary intelligence effort, a proclivity towards the current, and that largely a proclivity towards terrorism, is both being 'felt' and questioned by open source exploitation efforts. The author has suggested that the broader geo-political, socially constructed influences might be responsible for the ascendancy of this short-term approach. 'New risks' are perceived more significant than they really are. This in turn promotes a sincere yet superficial bias, which usurps an intrinsic, authentic desire to fundamentally examine them for legitimate potency at all.

The challenge for the intelligence community, put crudely, is that, where input to 'important' decision-making was once the sole preserve of the closed public traditional

intelligence function, now everyone can 'have a go'. Thus, there are two issues for the intelligence community as preferred supplier to decision makers. First, at the operational level: how best to now conduct open source exploitation for the benefit of the intelligence community given its demonstrable contribution. Second, at the political level, how to 'engage' with the variety of open source analysis generated outside the intelligence community in order to remain preferred supplier. The former requires a unified doctrine, training policy, and professional project establishing best practice. The latter requires a shift towards a notion of the intelligence community becoming a sound arbiter in the battle of ideas and arguments over strategy that incorporates more of the externally generated thinking than excluding it. This in turn suggests that the intelligence community has a purpose, and that this purpose is not unreasonably aligned to the political purpose of the day.

6.5 Further research

Inevitably, research of this nature throws up further questions that are simply beyond the scope of the original work. They are presented briefly here and may prove to be useful start points for further enquiry either internally by the intelligence community itself or by external bodies.

- Can the high order factors identified be meaningfully ranked?
- Can the efficacy of open source exploitation be genuinely measured or are internally-servicing targets and metrics rather than externally presented meaningful outcomes the only way?
- What would be the impact upon analysts and analytical product were they to undertake both closed analysis and open source exploitation simultaneously?
- Might a re-balancing of intelligence collection towards open source exploitation engender a more ethical intelligence conduct by reducing the reliance upon secret methods and a secretive culture?

- Will the democratisation of information precipitated by the opportunity for open source exploitation across the security commons lead to a multiplicity of 'truths' rather than an authoritative nation-state one? How should the intelligence community address the question - which truth, to which power, about what, by whom?
- What are the implications for open source exploitation and intelligence more broadly as copyright, intellectual property rights, and privacy regulation adjust to the ICT transformation?[3]
- The research has principally concentrated upon US, UK and multi-national organisation within the intelligence community. It would be instructive to understand how countries and organisations without similar recourse to closed intelligence collection conduct their intelligence functions, and whether that conduct of necessity includes a greater emphasis upon open source exploitation.

6.6 The changing same story

Open source intelligence remains as originally defined - the exploitation of open sources of information for intelligence purposes. Yet, open source has itself migrated in the lifetime of this research. The sources for and tools of exploitation are themselves transforming. Together with media product, grey literature, expert witness, and commercial product, one must now add the new social media class of blogs, wikis and other social software that are constructing the phenomenon of user generated content. Not only do these present sources of information for intelligence collection, as well as tools to aid analysis, they also combine and conspire to create another representation of reality alongside journalism, academia and intelligence. It will be interesting to watch.

Similarly and relatedly, beyond merely open source intelligence, a wider interpretation of open source is expanding into a movement pricking the public consciousness. The releasing of sections of the electromagnetic spectrum into the public domain and the burgeoning of open source software combined with open source information prefigures a

consensus concerned with openness and its significance for good governance. Yet the consensus is querulous. Notions of freedom of information enshrined in law are juxtaposed with the re-classification of information once public. Again, at the time of concluding this research, 'Wikileaks', an organisation representing the very epitome of open source tools attempting contextual understanding, has been launched to encourage 'leaking' in the so-called pursuit of open government; as if that action alone automatically confers better government.[4]

Put simply, more people can know more things more quickly - seemingly. Seemingly, because the democratisation of information is itself only a character change for politics rather than any fundamental change to its nature and purpose. Exhorting that good governance is best achieved in a frenzied public glare rather than the privacy of considered deliberation is merely a modern incarnation of former dénouements in the institution of trust between powerful elites and the rest. The nature of politics, like the nature of intelligence, which serves it, has not changed. Best judgements based upon best representations of reality in conditions of uncertainty and finite resource for purposeful ends will still have to be made. This depends upon the best information being collected and then interpreted by the best analysts. These resources no longer reside predominantly within the intelligence community; if they ever did. However, they are increasingly being harnessed by the intelligence community, perhaps more loosely and with greater difficulty than before thanks to the increasing commercialisation of such activity. Open source exploitation is no exception. Purpose will continue to be dissembled by the interplay between power, personalities and principal in the mix that is politics. A significant challenge for politics, and thus intelligence, is whether the Enlightenment ideal of pursuing universal truths, however illusive, will trump the cultural relativism that is considered by many to be sending us sleep-walking into the more serious chaos of absence of political purpose. Unfortunately, the elites have yet to master the means that cultural relativists seem to be dominating, and regain politics as power for purpose rather than simply for power.

So, concepts like user-generated content or 'Web 2.0' and the 'semantic Web' by no means herald the end of intelligence. Jimmy Wales, the founder of Wikipedia, puts it best himself when he cautions that everyone can tell jokes, but we still seem to need professional comedians.[5] The same might be said for journalists, academic researchers, and intelligence analysts. It is not the information that is singularly crucial, but what is made of it. The output of opinion is more likely to expand than decline, but who determines which opinion becomes policy, doctrine, or principle will hopefully remain the preserve of wise judgement. The danger of connoting open sources of information with 'digital solipsism' is to misunderstand the nature of open source exploitation for intelligence purposes.

Finally, and commensurate with Scott and Jackson, intelligence cannot be examined in the absence of its relationship to power and thus politics. The post 1989 geo-political security position defined by US hegemony and aided by its coalition allies has most influenced the conduct of the contemporary intelligence function; certainly for the US and UK if not also, to some degree, for their allies. However, deeper and longer socio-cultural trends have shaped a more fundamental context that has found powerful means of expression via the recent transformation in ICT. In this new context, characterised by globalisation, risk society, and changing societal expectation, wars against adversaries can only be won if battles for ideas, principles, and values are won first.

6.7 So what?

> "Everything should be open rather than closed and not the other way around"
>
> Senior UK Intelligence Professional[6]

There is nothing new in exploiting open sources of information. However, the quality, quantity, and availability of open sources of information are certainly of a different order than ever before. The contemporary transformation in ICT has transformed their scale and immediacy. Intelligence communities, amongst others, have recognised the contemporary

incarnation of the phenomenon through the formal establishment and incorporation of discrete open source exploitation efforts. In this regard it does represent a significant shift in the contemporary character and conduct of intelligence. But, open source exploitation does not represent a change in the nature of intelligence. That remains extant as support to decision-making and action.

By the same token, the nature of information does not change simply because of its provenance, whether classified, security protected, or bought from the local newsagent. The same fundamental rules apply. Whether information is found on the Internet, read in an obscure peer-reviewed journal in a rare language, or derived from agent émigrés, its integrity, authenticity and assurance, amongst other attributes, should be rigorously interrogated. And, of course, this is all before it is subsequently analysed, assessed, judged and utilised by policy makers with their own attendant human frameworks and frailties.

Yet, this relatively recent expansion in the incorporation and exploitation of open sources by secret intelligence communities does challenge the conventionally and traditionally held definition of intelligence as secret state activity to understand and influence foreign entities. It usefully exposes it as simply a definition of one type of intelligence conduct - espionage - so that a more comprehensive understanding of the contemporary purpose of intelligence might be pursued.

On one level, such clarification and pursuit of meaning is important because deeper more powerful influences, sponsored by the transformation in ICT, are at play. These influences, like globalisation and risk society, are changing the context which intelligence works in, but simultaneously trying to understand. Not only has the transformation in ICT re-energised the phenomenon of open source, but also its ability to mobilise changing societal expectations has intensified notions of openness, which intelligence is equally pressured to conform to. On another level, as intelligence communities struggle to harness the potential of contemporary ICT, the culture and structure of secrecy and security, which legitimately characterises parts of the intelligence function, are also arraigned to constrain

the intelligence benefits of OSINT. Thus, a paradox, between secrecy being the exclusive definition of intelligence and intelligence increasingly dependent upon open sources, has yet to be resolved.

Fundamentally, from a policy point of view, the principle question for the future of open source exploitation within intelligence communities is largely one of resource allocation. Inextricably tied-up in that question is: where should open source exploitation reside; how can relative effectiveness compared to closed be determined; and how is it best exploited? Why it should be done at all is answered by the model that this research effort has constructed; and that may inform these more important questions.

6.8 Recommendations

> "… to make recommendations to the Prime Minister for the future on the gathering, evaluation and use of intelligence …"[7]

The author makes one principal recommendation and nine other recommendations for open source exploitation policy. The principle recommendation - a National Open Source Council - might very well be the key to unlock the other nine, and is thus given prominence. The recommendations, most closely fit, and are broadly directed at the UK; although variations to suit the cultural, structural, technical and resource contexts of other nation-states and intelligence communities might usefully be extrapolated. They are as follows:

- **Establish a National Open Source Council**

  The principle recommendation is the establishment of a permanent, stand-alone, national open source council to coordinate and direct open source exploitation - policy, doctrine, training, standards and collection - across society on behalf of government.

It is **not** considered that this should constitute an intelligence agency in its own right in the sense that it is a self-contained organisation that conducts all national open source exploitation. Because open source has so thoroughly pervaded and percolated the intelligence community, and because open source exploitation so fundamentally supports all the other policy-advising systems, including closed intelligence, it would be unlikely that a central agency would cope with the nuanced, varied and bespoke requirements set for analysts at the point of production from the remote position of a separate agency. However, such an organisation should have an appropriate status, in the sense of being a self-directing and independent body responsible for open source exploitation as practice, in order to reflect the significance of a meaningful change from the *status quo ante*. Equally, it should be the fallback position for its own dispersed profession in terms of exploitation not otherwise possible at the 'coalface'. Significantly, such a national body should be deliberately placed outside the closed intelligence community: partly so that it might conduct its work with the minimum of secrecy or security restraint; partly so that it is seen as genuinely independent of any particular agency; partly so that it can interact and respond with a broader societal security commons; and partly to develop the particular contribution that open source brings to decision-making. Thus, it would probably be a mistake to follow the US example, which has set their lead open source organisation within an existing agency. Although, the OSC is part of the DNI it remains physically and firmly housed and 'controlled' within the CIA. However convenient that might be, the cultural influences and community perceptions do not correspond to genuine independence. Furthermore, because of cultural, structural and resource proclivities (let alone historical) there is a recognition that the vast difference in scale between the US IC and the rest militates against a one-size fits all approach to intelligence. It may be more likely that a one-size approach more closely fits 'the rest'. The US OSC has the capacity and capability to undertake open source exploitation in its own right on behalf of its IC as a distinct agency. Whether it can fulfil the cultural requirements remains to be seen. The UK experience, borne partly of necessity, but also from trial and error, indicates that the

dispersal of open source expertise as far out to the leading edge of analytical production as is possible is more effective.

It seems sensible to suggest that such a body should be based upon the UK's existing OSJWG, itself now expanded in recent years beyond the initial SIA plus DIS, and now SOCA, but also more seasoned open source practitioners such as BBC Monitoring as well as other relevant contributors from the private sector. Such an expanded OSJWG should simply be made 'permanent' as the professional 'head' of the open source community leading a national open source exploitation endeavour. There are several benefits to this arrangement over the informal arrangement to date. First, it would 'free-up' the current open source champion in Cabinet Office to concentrate upon her primary role of PHIA. Second, it would place the discipline in the hands of senior practitioners. Third, it would formally recognise the already informally acknowledged efficacy of open source exploitation as a distinct discipline. Fourth, it would 'free-up' the OSJWG to develop the discipline on a professional and permanent basis rather than as a secondary function to their already busy day jobs. Fifth, it would provide at least one alternate channel down which intelligence requirements might be set in the first place, as PHIA has mooted. Finally, as we migrate from a nation-state defence-oriented world to more collaborative global security efforts, it would prove a useful national asset to offer advice to nation-states, who do not necessarily have the luxury of closed resources or prefer not to use them, but need to be informed as best possible about the variety of risks that all states engage with.

It seems unlikely that the challenge of the exploitation of information found in the public domain is going to diminish. Thus, it would seem appropriate to put the best practitioners in control. In line with the findings of this research it may be important to include closed intelligence experience within such a body until such times as intelligence has internalised the broader contextual shift away from clandestine activity as its defining role towards the more inclusive necessity to support decision making.

- **Establish fundamental 'buy-in' and resource support**

  For all open source exploitation efforts, whether at a national level or intra-organisation, some key underlying fundamentals are pertinent to its establishment at the outset. First, there must be 'board-level' buy-in to reflect genuine support for any such enterprise. Second, and following on from the first, sufficient resource should be placed to allow open source exploitation to succeed rather than sufficient rope to let it hang. Third, if the resource does not reflect the basic composition of a typical open source cell then this research tends to show that it would be better for all not to bother.

- **Establish a basic exploitation structure**

  As a guide, an open source cell needs to address seven key features that characterise successful open source exploitation: intelligence direction; research expertise; commercial acumen; ICT support; knowledge working; digital media search; non-digital collection. Fundamentally implicit in the research element is a combined linguistic and cultural expertise. It is presumed that, like the ASD or BBC Monitoring, research analysts have language, cultural, and research expertise in one person. For certain requirements and targets one might equally engage technical rather than cultural expertise.

- **Aim for an 'all-source open source' capability**

  Open source exploitation mirrors and pursues all elements of the intelligence cycle from collection to analysis; mistakenly perceived exclusive to closed intelligence. It can collect across a variety of sources (media, grey, commercial, human), in digital and analogue format that reflect if not mirror closed collection methods. It can analyse across them in its own 'all-source open source' way. In some case-studies examined in this research, the ability to analyse is already undertaken, in others it is possible but not allowed, and in others it is not possible in the absence of cultural, linguistic, technical or collection expertise. With the proper resourcing, open source exploitation efforts can formulate alternative analysis and competing hypotheses for policy-makers. Arguably, open source exploitation, more than any other intelligence effort with the exception of

all-source analysis (which of course should include open), can influence policy in the sense of contributing to debate about what 'requirements' should be.

- **Open source process as 'push plus core'**

  Within an organisation that exploits open source, its practitioners should maintain both a centralised core for coordination, direction and organisational focus, as well as a dispersed workforce that can sit alongside (literally) analysts at the point of production. This process essentially reflects the 'push' principle rather than 'pull' approach towards information flow. It depends upon a hybrid approach to distributing open source expertise. This research indicates that, where open source is exploited within organisations at the 'leading edge' of the organisation's production effort supported by a central core of expertise, rather than all expertise entirely hidden away at the centre, it is positively regarded and actively demanded. One might usefully transpose the word 'push' for 'available' and 'pull' for 'unavailable'. Interestingly, the dilemma of pushing versus pulling information is also felt by organisations that are already independent open source exploitation efforts in their own right. Organisations like ASD, BBC Monitoring, and the agencies represented by the OSJWG continuously engage with their customers in order to establish precisely what they require from them and place their personnel in customer organisations to facilitate that.

- **Demonstrate relative efficacy**

  Given the imbalance between OSINT contribution to final product and resource allocation, let alone cultural and structural barriers to open source exploitation, it seems inevitable that open source exploitation efforts will need to establish metrics that reflect their relative contribution to the broader intelligence effort. Part of that evaluation might utilise the model proposed in this research, although the model is specifically directed at describing the precise contribution of open source rather than intelligence across the board. Yet, it ought to be necessary to coordinate metrics across the intelligence community, including open source exploitation, which more usefully reflects where response to requirement is best met. This might in turn more usefully

guide the allocation of resources across the community and government as a whole. While metrics best represent internally-facing comparisons of effectiveness, they merely represent efficiency measures when viewed from an external position. An effort to establish efficacy does not excuse external polities from establishing the objectives that decision makers and their advisors (including the intelligence community) should be aiming towards.

- **Determine appropriate resource allocation**

  Following on from the last point, the intelligence community should undertake further study to determine whether the balance of resource currently set genuinely reflects the relative contribution of the varying intelligence disciplines and agencies. Whilst this research has not been interested in resource allocation *per se*, it has been difficult not to observe that an anomaly exists between the claimed contribution and dedicated resource of open source intelligence. It should be explored at least.

- **Delineate current from longer-term open source exploitation**

  Some effort needs to be made in delineating current from longer-term open source intelligence requirements. Expeditionary engagements or crisis events that by their nature demand a surging of current intelligence requirements are most likely to be dominated by open source exploitation. This in turn might necessitate a different process and structure to longer-term open source exploitation, where the permanency of the organisation and its objectives dictate a different approach. However, this is not an issue peculiar to open source intelligence alone, but intelligence more widely.

- **Establish network architecture to disseminate open source product**

  In the absence of a functioning IC-wide IT architecture to facilitate communication, the establishment of an unclassified system like the US Intelink-U system, which carries open source exploitation, should be established until such times as open source product can be placed upon new secure networks as they becomes available. If banking can be done safely on line then, in principle, open source exploitation ought to be,

notwithstanding the fact that zero risk of compromise can never be guaranteed. The greater cost is not having the facility at all. This already happens in the US with SIPRNET and JWICS, and to a degree in the UK, where open source product is placed onto classified networks in order that they are made available and searchable to analysts at one single, central point.

- **Embark upon a professional project for open source exploitation**
  Finally, the open source community should consider embarking upon a professional project that establishes its practice upon a professional basis including: an educational discipline; a code of standards and ethics; the creation of a body of knowledge; certification of competencies; and a recognised forum for discussion. Furthermore, such professionals might be posted and promoted around the intelligence community as practitioners of a discrete discipline, much as the OSC are already doing via the nascent establishment of career OSINT Officers in the US intelligence community.

6.9 Contribution to knowledge

There is little or no substantive body of academic research work on the exploitation of open source for intelligence purposes beyond the odd peer-reviewed paper or book chapter. There is a vast practitioner literature, although it has largely been dominated by a tireless but somewhat evangelical single canon of work. In contemporary times, 2005 was a pivotal year for the formal exploitation of open sources within intelligence communities as other work became increasingly available, pursuant to increased attention, practical and theoretical, to open source exploitation. By contrast, there is considerable and varied academic work on the broader subject of intelligence - as understood in terms of government purposes. It has been conducted principally from the purviews of political science and historical analysis. All of this enquiry has been invigorated by 9/11 and the question of 'Iraqi WMD' in order to re-focus upon the purpose of intelligence in the contemporary world. This research has contributed to both camps.

There are five ways in which this research represents a contribution to knowledge:

- It is the first time that academic research has been conducted into the exploitation of open source intelligence within and across public intelligence and security agencies.
- It establishes a model describing the high order contributing factors of this exploitation to the broader intelligence function within those agencies.
- It makes some recommendations towards national policy and doctrine for open source exploitation based upon the findings of the research.
- It posits that open source exploitation - itself a reflection of the changing contemporary environment - might usefully form the lens through which the intelligence community can understand a changing world if not itself.
- It makes some contribution to a theory of intelligence by drawing distinction between the nature and character of intelligence, and then further contends that notions of secrecy and the cultural fascination with classification should no longer dominate the classic definition of intelligence in contemporary times.

In short the background theory of open source exploitation is now placed upon a firmer footing through the focal theory of this research than it was before.

6.10 Conclusion

> "…(T)he study of intelligence must strive to become more self-consciously analytical and theoretical than hitherto, because it is so significant for both domestic and international security."
>
> Gill and Phythian, 2006[8]

This thesis started by asking the question how the contribution of open source exploitation to intelligence might be described by a set of high order factors. Essentially the research shows that it changes the character of intelligence at the operational level by uniquely contributing support to decision-making via the high order factors described: context;

utility; focus; surge; communicability; cross-check; and analysis. Furthermore, these factors usefully differentiate open source contribution from closed. On another level, it also facilitates intelligence's understanding of context, in the sense of understanding the significant shapers of context including globalisation, risk society, and changing societal expectation. In this way it can reflexively contribute to intelligence an understanding of itself and the subjects it ought to be attempting to understand.

The new question at an operational level is how intelligence, as currently represented by public sector agencies conducting predominantly clandestine espionage, can best harness this changing character should they wish to - structurally, culturally and financially - in order to remain a principal and principled provider of support to decision-making. This may require demonstration of the internal relative effectiveness of the various intelligence disciplines and agencies, to which this thesis has contributed some factors for consideration. At the contextual level, a more troublesome question emerges in regard to intelligence's relationship with politics - which truth, to which power, about what, by whom. Security is intrinsically, essentially, and ultimately about people; yet, their intentions and behaviours remain mysterious.

> "One of the most worrying things … was how arbitrary are the processes of decision-making, how subject to the vagaries of group and individual psychology … how random it is. Deciding policy is terrifyingly at the mercy of human vagaries."[9]

> "If there is a crisis of trust in our society, there is only one known potential remedy, and to the chagrin of many it is at the micro-level of individual behaviour, rather than at the macro-level of social-engineering. It is for us to attempt to be trustworthy, to the best of our abilities. And even that might not work."[10]

The research aim was stated as an enquiry into the contribution of open source exploitation to the broader intelligence function. Now, a net has been cast in the form of a model, which describes that contribution, in the hope of catching as many 'fish' that fit the net as possible.[11]

References and Notes:

[1] Scott, L., Jackson, P., 2004, 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security*, 19, 2, pp.139-169.

[2] Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press, p.29.

[3] See the recently published Gower Report for development of this area, available at: http://www.hm-treasury.gov.uk/independent_reviews/gowers_review_intellectual_property/gowersreview_index.cfm

[4] http://www.wikileaks.org/

[5] BBC Radio 4, the PM Programme, 2 January 2007.

[6] This view was expressed in the conclusion to a presentation on the UK's Intelligence Machinery process by a very senior UK intelligence practitioner under Chatham House rules at St Anthony's College, Oxford, February 2007.

[7] Part of the Terms of Reference paragraph, which begins the Butler Review, in: UK Privy Councellors, 2004, *Review of Intelligence on Weapons of Mass Destruction (The Butler Review)*, House of Commons, HC 898, p.1.

[8] Gill, P., Phythian, M., 2006, *op cit*, p.172.

[9] From an interview with a senior UK Government adviser to Prime Minister Blair quoted in: James, O., 2007, *Affluenza*, London: Vermilion, pp.328-329.

[10] O'Hara, K., 2004, *Trust: From Socrates to Spin*, Cambridge: Icon Books.

[11] Popper, K., 1935, *The Logic of Scientific Discovery*, Abingdon: Routledge.

BIBLIOGRAPHY

Primary sources (Interviews):

The following primary source references refer to the notes from the semi-structured interviews conducted with case study representatives. All interviews were conducted in the absence of recording equipment given the nature of the subject and the location of the interviews. They were all transcribed immediately following the interviews. All interviewees were conducted under the condition of anonymity, but recognising the organisation with which they were engaged. The semi-structured interviews followed the template in Appendix A, but, essentially, discussion revolved around three key questions:

- Why do you do what you do (open source exploitation)?
- How do you do what you do?
- So what?

It is also important to note that the interviews did not represent the end of dialogue. In many cases, there has been additional - some brief, some continuous - communication with many of the interviewees and most of the institutions, notably the UK OSJWG. In other cases there has been extensive communication too nuanced and extensive to record in detail; for example with BBC Monitoring, Hazard Management Solutions, Political Risk Associates, members of the Oxford Intelligence Group, and the Asian Studies Detachment.

DIS 1, 2003, interview with the former Head of the UK Defence Intelligence Staff Open Source Centre, conducted at the UK Ministry of Defence Old War Office Building, London, on 3 March 2003.

DIS ANON R1, 2005, interview with a then UK Defence Intelligence Staff analyst, in London, on 20 October 2005.

DIS ANON R2, 2005, interview with a just retired analyst, UK Defence Intelligence Staff analyst, in Shrivenham, on 28 October 2005.

EUROPOL 1, 2003, interview with a then EUROPOL analyst (Corruption & Organised Crime), at EUROPOL, Den Haag, between 16-18 April 2003.

EUROPOL 2, 2003, interview with a then EUROPOL analyst (Serious Crime), at EUROPOL, Den Haag, between 16-18 April 2003.

EUROPOL 3, 2003, interview with a then EUROPOL analyst (Eastern European Crime and EU Computer Related Crime), at EUROPOL, Den Haag, between 16-18 April 2003.

EUROPOL 4, 2003, interview with the then Head of EUROPOL's Counter Terrorism Cell, at EUROPOL, Den Haag, between 16-18 April 2003.

EUROPOL 5.1, 2003, first interview with the then Head of EUROPOL's Open Sources & Documentation Unit (Open Source Cell), at EUROPOL, Den Haag, Between 16-18 April 2003.

EUROPOL 5.2, 2007, second interview with former Head of EUROPOL's Open Sources & Documentation Unit (Open Source Cell), by telephone, 4 January 2007.

EUROPOL 6, 2003, interview with a then analyst (Immigration and Refugees), at EUROPOL, Den Haag, between 16-18 April 2003.

EUROPOL 7, 2003, interview with a then analyst (Serious Crime), at EUROPOL, Den Haag, between 16-18 April 2003.

ICTY 1-4, 2003, collective interview with four Research Officers with the Office of the Prosecutor in the UN International Criminal Tribunal for the Former Yugoslavia (ICTY), at the ICTY, Den Haag, between 16-18 April 2003.

ICTY 5, 2003, interview with the then Military Analysis Team Leader with the Office of the Prosecutor in the UN International Criminal Tribunal for the Former Yugoslavia (ICTY), at the ICTY, Den Haag, between 16-18 April 2003.

ICTY 6, 2002, interview with the Director of the Research Office with the Office of the Prosecutor in the UN International Criminal Tribunal for the Former Yugoslavia (ICTY), at the ICTY, Den Haag, between 20-23 November 2002.

BBC-M 1, 2002-2006, ongoing discussion and several site visits with the then Customer Services Director for BBC Monitoring.

BBC-M 2, 2002-2006, ongoing discussion and several site visits with the Head of Business Development and Customer Relations for BBC Monitoring.

HMRC 1, 2002, interview with the then Head of Intelligence Analysis, Law Enforcement Division for the then UK's HM Customs & Excise, at HM Customs Headquarters London, 27 November 2002.

ACADEMIA 1, 2005, interview with the Director of the Conflict Studies Research Centre at the Defence Academy of the UK, at Shrivenham, 10 June 2005.

SOCOM 1, 2006, interview with the then Director of the US Special Operations Command (SOCOM)'s Open Source Exploitation Branch, at MacDill US Air Force Base, Tampa (FL), between 18-20 April 2006.

COAS 3, 2007, interview with an Intelligence Director in the UK Government Cabinet Office Assessments Staff (COAS), at Cabinet Office, Whitehall, London, 19 January 2007.

OSJWG 1, 2005, collective discussion with the UK's Open Source Joint Working Group, at GCHQ Cheltenham, 15 December 2005.

OSJWG 2, 2007, collective discussion with the UK's Open Source Joint Working Group, at GCHQ Cheltenham, 28 March 2007.

PIB 1 ('Political Risk Associates'), 2005, Private Information Broker (Protest & Pressure Groups - Animal Rights), at their offices (and subsequent correspondence), 7 September 2005.

PIB 2 (Hazard Management Solutions), Private Information Broker (Improvised Explosive Devices) throughout 2002-2007.

PIB 3 (Exclusive Analysis), Private Information Broker (Political and violent risk), at their offices throughout 2004-2006.

SIP 1, 2005, discussion with former US Deputy Assistant Director of Central Intelligence for Analysis and Production, CIA, at Oxford Intelligence Group meeting, 5 December 2005.

ASD 1, 2007, joint interview with the Director & Operations Division Chief, US Army's Asia Studies Detachment, Camp Zama, Japan, 29 January-2 February 2007.

ASD 2, 2007, interview with the Chief of the North East Asia Branch, US Army's Asia Studies Detachment, Camp Zama, Japan, 29 January 2007.

ASD 3, 2007, interview with the Branch Chief and Deputies of the South Asia/South East Asia/Global War on Terrorism Branch, US Army's Asia Studies Detachment, Camp Zama, Japan, 30 January 2007.

ASD 4, 2007, interview with the Section Chief of the Current Operations Section, US Army's Asia Studies Detachment, Camp Zama, Japan, 30 January 2007.

ASD 5, 2007, interview with the Battalion Commander US Army's 441st Military Intelligence Battalion, US Army's Asia Studies Detachment, Camp Zama, Japan, 2 February 2007.

ASD 6, 2007, collective meeting with the 'Tokyo Office', US Army's Asia Studies Detachment, Camp Zama, Japan, 1 February 2007.

Secondary sources (Literature)

Ackerman, R.K., 2006, 'Intelligence Center Mines Open Sources', *SIGNAL Magazine*, March 2006,

Adams, J., 1995, *Risk*, London: UCL Press, ISBN: 1-85728-068-7.

Adams, J., 1996, *Cars, Cholera and Cows: Virtual Risk and the Management of Uncertainty*, Manchester: Manchester Statistical Society, ISBN: 0-85336-135-5.

Aftergood, S., Report No: 71, 1997, *Secrecy & Government Bulletin*, Federation of American Scientists, Washington.

Aftergood, S., 2005, *The Age of Missing Information: The Bush Administration Campaign against openness*, 17 March 2005.

Aldrich, R., 2002, 'Grow Your Own: Cold War Intelligence and History Supermarkets', *Intelligence and National Security*, 17, 1, pp.135-152.

Aldrich, R.J., 2005, 'Setting Priorities in a World of Changing Threats', *NATO Workshop on Intelligence Reform*, St Anthony's College, Oxford, 11 November 2005.

Aldrich, R.J., 2004, 'Transatlantic Intelligence and Security Cooperation', *International Affairs*, 80, 4, pp.731-753.

Aldrich, R.J., 2005, 'Whatever Happened to the Old New Threats? Setting Priorities in a World of Global Change', 10 December 2005, UK Defence Academy.

Aldrich, R.J., 2005, 'Whitehall and the Iraq War: The UK's Four Intelligence Enquiries', *Irish Studies in International Affairs*, 16, 2005, pp.73-88.

Alexander, C., (Ed), 2000, *Visions of Risk*, London: Pearson Education, ISBN:0-877-78320-9.

Andregg, M., 2003, 'How "Wisdom" Differs from Intelligence and Knowledge', *Intelligence Studies Section of the International Studies Association*, Portland (OR), USA, 28 February 2003.

Andregg, M., 2002, 'The Primary Value of Restoring a Healthy Relationship Between Intelligence Agencies and the Academic World is a Revolution in Intelligence Affairs', *Intelligence Studies Section of the International Studies Association*, New Orleans, USA, 25 March 2002.

Angell, I., 2000, *The New Barbarian Manifesto: How to Survive the Information Age*, London: Kogan Page, ISBN: 0-7494-3505-4.

Arnold, S., 2003, 'The Other Intelligent Open Source', *Webactive Magazine,* available at: http://www.webactivemagazine.co.uk/information-world-review/features/2084026/intelligent-open-source

Arnold, S.E., 2005, *The Google Legacy: How Google's Internet Search is Transforming Application Software*, Tetbury: Infonortics, accessible at: http://www.infonortics.com/publications/google/google-legacy.html

Atlee, T., 2003, *The Tao of Democracy*, Cranston: The Writers' Collective, ISBN: 1-932133-47-X.

Baird, Z., Barksdale, J., Report No: 2, 2003, *Creating a Trusted Network for Homeland Security*, Markle Foundation: Task Force on National Security in the Information Age, New York, available at: http://www.markletaskforce.org/Report2_Full_Report.pdf

Ball, D.J., Report No: 426/2002, 2002, *Playgrounds - Risks, Benefits and Choices*, Health & Safety Executive, London.

Barber, B.R., 2003, *Jihad vs. McWorld: Terrorism's Challenge to Democracy*, London: Corgi Books, ISBN: 0-552-15129-7.

Barber, J., 2001, 'An Intelligence, surveillance and reconnaissance (ISR) Vision for the Canadian Forces', *Canadian Military Journal*, Winter, pp.41-46.

Barger, D., 2005, *Toward Revolution in Intelligence Affairs*, RAND, Arlington, VA.

Barnett, R., 2000, 'Thinking the University, Again', *Educational Philosophy and Theory*, 32, 3, pp.319-326.

Barnett, R., 2000, 'University Knowledge in an Age of Supercomplexity', *Higher Education*, 40, pp.409-422.

Barnett, R., 2000, 'Supercomplexity and the Curriculum', *Studies in Higher Education*, 25, 3, pp.244-265.

Barnett, R., 1990, *The Idea of Higher Education*, Buckingham: Open University Press, ISBN: 0-335-09420-1.

Bate, R., 1999, *What Risk?: Science, Politics & Public Health*, Oxford: Butterworth-Heinemann, ISBN: 0-7506-4228-9.

BBC News, 2005, *Iraq Dossier Prompts Rule Change*, available at: http://news.bbc.co.uk/1/hi/uk_politics/4375241.stm

Bean, H., 2007, 'The DNI's Open Source Center: An Organizational Communication Perspective', *International Journal of Intelligence and CounterIntelligence*, 20, 2, pp.240-257.

Beck, U., 1999, *World Risk Society*, Oxford: Blackwell, ISBN: 0-7456-2220-8.

Beck, U., 1992, *Risk Society: Towards a New Modernity*, London: Sage Publications, ISBN: 0-803-98346-8.

Belasco, J.A., Stayer, R.C., 1995, *Flight of the Buffalo: Soaring to Excellence, Learning to Let Employees Lead*, Boston, MA: Little, Brown and Company, ISBN: 0-446-67008-1.

Berkowitz, B.D., Goodman, A.E., 2000, *Best Truth: Intelligence in the Information Age*, London: Yale University Press, ISBN: 0-300-09397-7.

Berkowitz, B.D., 2003, 'The DI and IT: Failing to keep up with the information revolution', *Studies in Intelligence: Journal of the American Intelligence Professional*, 47, 1, pp.12-13.

Berners-Lee, T., Hendler, J., Lassila, O., 2001, 'The Semantic Web', *Scientific American*, 284, 5, pp.34-44.

Bernstein, P.L., 1996, *Against the Gods: The Remarkable Story of Risk*, New York: John Wiley & Sons, ISBN: 0-471-29563-9.

Best, R.A., Report No: RL 33539, 2006, *Intelligence Issues for Congress*, US Congressional Research Service, Washington.

Better Regulation Commission, 2006, *Risk, Responsibility and Regulation: Whose Risk is it Anyway*, Better Regulation Commission, London, available at: http://www.brc.gov.uk/publications/risk_report.asp

Betts, R.K., 2002, 'Fixing Intelligence', *Foreign Affairs*, January/February 2002.

Betts, R.K., 1978, 'Analysis, War, and Decision: Why Intelligence Failures are Inevitable', *World Politics*, 31, 1, pp.61-89.

Bhagwati, J., 2004, *In Praise of Globalization*, New York: Oxford University Press, ISBN: 0-19-517025-3.

Björe, M., 1995, *Six Years of Open Source Information: Lessons Learned*, 12 Dec 2003.

Blair, T., 2005, 'Risk and the State', 26 May 2005, Institute of Public Policy Research, available at http://www.number-10.gov.uk/output/Page7562.asp

Blair, T., 2006, *A Global Alliance for Global Values*, dated: September 200635, London, Foreign Policy Centre, ISBN: 1-905833-06-7.

Bloom, H., 2000, *Global Brain: The Evolution of Mass Mind From the Big Bang to the 21st Century*, New York: John Wiley & Sons, ISBN: 0-471-41919-2.

Bonoma, T.V., 1985, 'Case Research in Marketing: Opportunities, Problems, and a Process', *Journal of Marketing Research*, 22, May, pp.199-208.

Bookchin, M., 1995, *Re-enchanting Humanity: A Defense of the Human Spirit Against Anti-humanism, Misanthropy, Mysticism and Primitivism*, London: Cassell, ISBN: 0-304-32839-1.

Borge, d., 2001, *The Book of Risk*, New York: John Wiley & Sons, ISBN: 0-471-32378-0.

Borodzicz, E., 2005, *Risk, Crisis and Security Management*, Chichester: John Wiley & Sons, ISBN: 0-470-86704-3.

Borodzicz, E.P., Gibson, S.D., 2006, 'Corporate Security Education: Towards Meeting the Challenge', *Security Journal*, 19, 3, pp.180-195.

Bowman, M.E., 2003, 'Some-Time, Part-Time and One-Time Terrorism', *Intelligencer, Journal of US Intelligence Studies*, 13, 2, pp.13-18.

Bowman, S., Willis, C., 2003, *We Media: How Audiences are Shaping the Future of News and Information*, July, 2003, Reston, VA, The Media Center at The American Press Institute, available at: www.hypergene.net/wemedia

Brand, S., 1998, 'Freeman Dyson's Brain', *Wired Magazine*, February 1998.

Briggs, R., (Ed), 2002, *The Unlikely Counter-Terrorists*, London: The Foreign Policy Centre, ISBN:1-903558-21-2.

Briggs, R., (Ed), 2003, *Doing Business in a Dangerous World*, London: The Foreign Policy Centre, ISBN:1-903558-30-1.

Briggs, R., 2004, *Doing Business in the New Global Security Environment*, DEMOS, London.

Bruneau, T.C., 2001, 'Controlling Intelligence in New Democracies', *International Journal of Intelligence and CounterIntelligence*, 14, 3, pp.323-341.

Bryant, D.J., Webb, R.D.G., McCann, C., 2003, 'Synthesizing two approaches to decision making in command and control', *Canadian Military Journal*, Spring, pp.29-34.

Bryson, B., 2004, *A Short History of Nearly Everything*, (Black Swan Edition), London: Doubleday, ISBN: 0-552-99704-8.

Burger, T.J., 2005, 'Opening Up the CIA', *Time*, 7 August 2005,, p.'Notebook'.

Burgess, A., 2004, *Cellular Phones, Public Fears, and a Culture of Precaution*, Cambridge: Cambridge University Press, ISBN: 0-521-52082-7.

Burns-Howell, T., Cordier, P., Eriksson, T., 2003, *Security Risk Assessment and Control*, Leicester: Perpetuity Press, ISBN: 1-899287-66-3.

Buruma, I., Margalit, A., 2004, *Occidentalism: A Short History of Anti-Westernism*, London: Atlantic Books, ISBN: 1-84354-287-0.

Byrd, S., 2004, *Independent Commissions on National Security Issues*, available at: http://www.fas.org/irp/congress/2004_cr/s030304.html

Cameron, C., 2004, *Flinging Open the Doors to Intelligence gathering*, available at: http://ojr.org/ojr/workplace/1097814155.php

Carroll, T.P., 2001, 'The Case Against Intelligence Openness', *International Journal of Intelligence and CounterIntelligence*, 14, 4, pp.559-574.

Cavaye, A., 1996, 'Case Study Research: A Multi-Faceted Research Approach for IS', *Information Systems Journal*, 6, pp.227-242.

Chalmers, A.F., 2005, *What is This Thing Called Science?*, (Third Edition), Maidenhead: Open University Press, ISBN: 0-335-20109-1.

Chang, Y., 2005, *Mao: The Unknown Story*, London: Jonathan Cape, Random House, ISBN: 0-224-07126-2.

Chapman, R.D., 1999, 'Reflections on Terrorism: A Sideline View', *International Journal of Intelligence and CounterIntelligence*, 12, 2, pp.207-226.

Charters, D.A., 2001, 'The Future of Military Intelligence within the Canadian Forces', *Canadian Military Journal*, Winter, pp.47-52.

Chomsky, N., 2004, *Hegemony or Survival: America's Quest for Global Dominance*, London: Penguin, ISBN: 0-141-01505-5.

CIA, 1971, *A Review of the Intelligence Community*, CIA, Washington.

CIA, 2001, *Are You Ready? Implications of a Changing Global Environment for Open Source Intelligence*, Global Futures Partnership in the Directorate of Intelligence, Washington.

Clift, A.D., 2003, 'From Semaphore to Predator: Intelligence in the Internet Era', *Studies in Intelligence: Journal of the American Intelligence Professional* 47, 3.

Coate, K., Barnett, R., Williams, G., 2001, 'Relationships Between Teaching and Research in Higher Education in England', *Higher Education Quarterly*, 35, 2, pp.158-174.

Cofflard, M., 2004, *L'Emir: La Peur Aura-t-elle le Dessus*, Paris: Fayard, ISBN : 2-213-61991-3.

Collis, J., Hussey, R., 2003, *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, (Second Edition), New York: Palgrave Macmillan, ISBN: 0-333-98325-4.

Cook, C., Thompson, B., 2000, 'Reliability and Validity of SERVQUAL Scores Used to Evaluate Perceptions of Library Service Quality', *The Journal of Academic Librarianship*, 26, 4, pp.248-258.

Cope, N., 2004, 'Intelligence Led Policing or Policing Led Intelligence?', *British Journal of Criminology*, 44, 2, pp.188-203.

Cornish, P., (Ed), 2007, *Britain and Security*, London: The Smith Institute, ISBN:1-905370-19-9.

Cornyn, J., 2004, 'Ensuring the Consent of the Governed', *LBJ Journal of Public Affairs*, Fall, pp.7-10.

Council of the European Union, Report No: 14469/4/05 REV 4, 2005, *The European Union Counter-Terrorism Strategy*, Council of the European Union, Brussels.

Covello, V., McCallum, D., Pavovla, M., (Ed), 1989, *Effective Risk Communication: The Role and Responsibility of Government and Non-Government Organizations*, New York: Plenum Press, ISBN:0-306-43075-4.

Craddock, P., 2002, *Know Your Enemy: How the Joint Intelligence Committee Saw the World*, London: John Murray, ISBN: 0-7195-6048-9.

Croom, H.L., 1969, 'The Exploitation of Foreign Open Sources', *Studies in Intelligence: Journal of the American Intelligence Professional*, 13, 2 Summer, pp.129-136.

Darke, P., Shanks, G., Broadbent, M., 1998, 'Successfully Completing case Study Research: Combining Rigour, Relevance and Pragmatism', *Information Systems Journal*, 8, pp.273-289.

Davenport, T.H., Prusak, L., 2000, *Working Knowledge: How Organizations Manage What They Know*, Boston: Harvard Business School Press, ISBN: 1-57851-301-4.

Davies, P., 2002, 'Ideas of Intelligence: Divergent National Concepts and Institutions', *Harvard International Review*, pp.62-66.

Davies, P.H., 2002, 'Intelligence, Information Technology and Information Warfare', *Annual Review of Information Science and Technology*, 36, pp.313-352.

Davies, P.H., 2005, 'A Critical Look at Britain's Spy Machinery', *Studies in Intelligence: Journal of the American Intelligence Professional*, 49, 4, pp.41-54.

Davis, 1995, 'Insightful Interviews: A Policymaker's Perspective on Intelligence Analysis', *Studies in Intelligence: Journal of the American Intelligence Professional*, 38, 5, pp.1-9.

Davis, D., 2001, *A Guide to Investigating Using the Internet*, Leicester: Perpetuity Press, ISBN: 1-899287-58-2.

Davis, I., 2005, 'The Biggest Contract', *The Economist*, 28 May 2005, pp.87-89.

Davis, J., 2003, 'Strategic Warning: If Surprise is Inevitable, What Role for Analysis?', *Kent Center Occasional Papers*, 2, January 2003.

de Botton, A., 2004, *Status Anxiety*, London: Penguin Books, ISBN: 0-241-14238-5.

De Jong, B., Platje, W., Steele, R.D., (Ed), 2003, *Peacekeeping Intelligence: Emerging Concepts for the Future*, Oakton, Virginia: OSS International Press, ISBN: 0-9715661-2-7.

Dearlove, R., Quiggin, T., 2006, *Contemporary Terrorism and Intelligence*, available at: http://www.isn.ethz.ch/news/sw/details.cfm?ID=16521

Deibert, R.J., 2003, 'Deep Probe: The Evolution of Network Intelligence', *Intelligence and National Security*, 18, 4, pp.175-193.

Deisler, P.F., 2002, 'A Perspective: Risk Analysis as a Tool for Reducing the Risks of Terrorism', *Risk Analysis*, 22, 3, pp.405-413.

Delves, C., 2006, 'RUSI-BAPSC First Annual Conference', 30 October 2006, Olive Group.

Denzin, N., Lincoln, Y., (Ed), 1993, *Handbook of Qualitative Research*, Thousand Oaks, CA: Sage Publications, ISBN: 0-803-94679-1.

Denzin, N., Lincoln, Y., (Ed), 1998, *Collecting and Interpreting Qualitative Materials*, Thousand Oaks, CA: Sage Publications, ISBN: 0-761-91434-X.

Devji, F., 2005, *Landscapes of the Jihad: Militancy, Morality, Modernity*, London: C. Hurst & Co, ISBN: 1-85065-775-0.

IAEA, D.G., Report No: GOV/2005/9, 2005, *Implementation of the NPT Safeguards Agreement in the Arab Republic of Egypt*, International Atomic Energy Authority, Vienna, available at: http://www.carnegieendowment.org/static/npp/Egypt_Feb_2005.pdf

Donald, D., 2006, Whitehall Paper 66, *After the Bubble: British Private Security Companies after Iraq*, London: Royal United Services Institute.

Donovan, L.A., 2005, 'Citizens as Intelligence Volunteers: The Impact of Value Structures', *International Journal of Intelligence and CounterIntelligence*, 18, 2, pp.239-245.

Dorn Walter, A., 1999, 'The Cloak and the Blue Beret: Limitations on Intelligence in UN Peacekeeping', *International Journal of Intelligence and CounterIntelligence*, 12, 4, pp.414-447.

Doswell, B., 2000, *A Guide to Business Continuity Management*, Leicester: Perpetuity Press, ISBN: 1-899287-57-4.

Doswell, B., Lilburn-Watson, D., 2002, *A Guide to Information Security Management*, Leicester: Perpetuity Press, ISBN: 1-899287-60-4.

Drucker, P.F., 'The Next Information Revolution', *Forbes ASAP*, August 1998, p 46.

Dupont, A., 2003, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, 18, 4, pp.15-39.

Durodié, W., 2004, 'The Limitations of Risk Management: Dealing with Disasters and Building Social Resilience', *Tidsskriftet Politik*, 8, 1, pp.14-21.

Durodié, W., 2005, *The Domestic Management of Terrorist Attacks*, Report No: L147251003, London, available at: http://www.terrorismresearch.net

Durodié, W., 2003, 'Limitations of Public Dialogue in Science and the rise of New 'Experts'', *Critical Review of International Social and Political Philosophy*, 6, 4, pp.82-92.

Durodié, W., 2004, 'Political Tunnel Vision is Today's Real Terror', *The Times Higher Education Supplement*, 26 March 2004.

Durodié, W., 2004, 'Sociological Aspects of Risk and Resilience in Response to Acts of Terrorism', *World Defence Systems*, 7, pp.214-216.

Durodié, W., 2004, 'Facing the Possibility of Bioterrorism', *Current Opinion in Biotechnology*, 15, pp.264-268.

Durodié, W., 2005, 'Risk and the Social Construction of 'Gulf War Syndrome'', *Philosophical Transactions of the Royal Society B*, 2006, 361, pp.689-695.

Durodié, W., 2000, Plastic Panics: European Risk Regulation in the Aftermath of BSE, in: *Rethinking Risk and the Precautionary Principle*, Morris, J., (eds.), London: Butterworth-Heinemann, pp: 140-167, ISBN: 0-750-64683-7.

Durodié, W., Wessely, S., 2002, 'Resilience or Panic? The Public and Terrorist Attack', *The Lancet*, 360, December 14, pp.1901-1902.

Eagleton, T., 2003, *After Theory*, London: Penguin Group, ISBN: 0-713-99732-X.

Easterby-Smith, M., Thorpe, R., Lowe, A., 1991, *Management Research: An Introduction*, (First Edition), London: Sage Publications, ISBN: 0-8039-8393-X.

Easterby-Smith, M., Thorpe, R., Lowe, A., 2002, *Management Research: An Introduction*, (Second Edition), London: Sage Publications, ISBN: 0-7619-7285-4.

Economist, 2005, 'America's Intelligence Reforms: Can Spies be Made Better?', *The Economist*, 19 March 2005, pp.29-31.

Economist, 2005, 'Britain's Intelligence Services: Cats' Eyes in the Dark', *The Economist*, 19 March 2005, pp.32-34.

Eisendrath, C., (Ed), 2000, *National Insecurity: US Intelligence after the Cold-War*, Philadelphia: Temple University Press, ISBN: 1-56639-848-7.

Eisenhardt, K.M., 1989, 'Building Theories from Case Study Research', *Academy of Management Review*, 14, 4, pp.532-550.

Exclusive Analysis, 2004, *Global Risk Outlook 2005*, Exclusive Analysis, London.

Federation of American Scientists, 2003, *National Security Language Act*, available at: http://www.fas.org/irp/congress/2003_cr/hr3676.html

Federation of American Scientists, 2003, 'Lost and Found', *Secrecy News Alert*, dated 12 December 2003.

Feldman, S., Marks V., 2005, *Panic Nation: Unpicking the Myths We're Told About Food and Health*, London: John Blake Publishing Ltd, ISBN: 1-84454-122-3.

Ferris, J., 2003, 'A New American Way of War? C4ISR, Intelligence and Information Operations in Operation 'Iraqi Freedom': A Provisional Assessment', *Intelligence and National Security*, 18, 4, pp.155-174.

Fingar, T., 2005, Department of State: Bureau of Intelligence and Research, *Security Threats to the United States*, Senate Select Committee on Intelligence, Washington DC, dated 16 February 2005.

Fischhoff, B., 2002, Assessing and Communicating the Risk of Terrorism, in: Teich, A., Nelson, D., Lita, S., 2002, (Eds), *Science and Technology in a Vulnerable World*, pp.51-64.

Fischhoff, B., Gonzalez, R., Small, D., Lerner, J., 2003, 'Evaluating the Success of Terror Risk Communications', *Biosecurity and Bioterrorism: Biodefense Strategy, Practice, and Science*, 1, 4, pp.255-258.

Florini, A., 2003, *The Coming Democracy: New Rules for Running a New World Order*, Washington: Island Press, ISBN: 1-55963-289-5.

Florini, A., 1998, 'The End of Secrecy', *Foreign Policy*, Summer, pp.50-64.

Florini, A., (Ed), 2000, *The Third Force: The Rise of Transnational Civil Society*, Washington: Carnegie Endowment for International Peace, ISBN: 0-87003-179-1.

Friedman, G., 2004, *America's Secret War: Inside the Hidden Worldwide Struggle Between the United States and its Enemies*, London: Doubleday, Random House, ISBN: 0-316-72862-4.

Friedman, R.S., 1998, 'Open Source Intelligence', *Parameters*, Summer, pp.159-165.

Friedman, T.L., 2006, *The World is Flat: The Globalized World in the Twenty-First Century*, London: Penguin Books, ISBN: 0-141-02272-8.

Fukuyama, F., 2002, *Our Posthuman Future*, London: Profile Books, ISBN: 1-86197-297-0.

Fukuyama, F., 1992, *The End of History and the Last Man*, London: Penguin, ISBN: 0-14-013455-7.

Furedi, F., 2002, *Culture of Fear: Risk-Taking and the Morality of Low Expectation*, London: Continuum, ISBN: 0-8264-5930-7.

Furedi, F., 2004, *Therapy Culture: Cultivating Vulnerability in an Uncertain Age*, London: Routledge, ISBN: 0-415-32159-X.

Furedi, F., 2004, *Where Have all the Intellectuals Gone? Confronting 21st Century Philistinism.*, London: Continuum, ISBN: 0-8264-6769-5.

Furedi, F., 2005, *Politics of Fear*, London: Continuum, ISBN: 0-8264-8728-9.

Furedi, F., 2005, *Why Do We Fear Freedom?*, available at: http://www.spiked-online.com/Articles/0000000CADC6.htm

Fyffe, G., 2003, 'Intelligence Sharing and OSINT', *Open Source Solutions 2003*, Washington DC, USA, 17 September 2003.

Gable, G., 1994, 'Integrating Case Study and Survey Research Methods: An Example in Information Systems', *European Journal of Information Systems*, 3, 2, pp.112-126.

Gannon, J.C., 2000, 'Address to the Washington College of Law at American University Washington DC', 6th October.

Gansler, J.S.L., Lucyshyn, W., 2004, *The Unintended Audience: Balancing Openness and Secrecy. Crafting an Information Policy for the 21st Century*, Centre for Public Policy and Private Enterprise, School of Public Policy, University of Maryland, September 2004.

Garrick, J.B., 2002, 'Perspectives on the Use of Risk Assessment to Address Terrorism', *Risk Analysis: An International Journal*, 22, 3, pp.421-423.

Gaskin, J.C.A., (Ed), 1998, *Leviathan: Thomas Hobbes*, Oxford: Oxford Paperbacks, ISBN: 0-192-834-983.

George, B., Button, M., 2000, *Private Security*, Leicester: Perpetuity Press Limited, ISBN: 1-8999287-70-1.

Gibson, S.D., 2005, 'In the Eye of the Perfect Storm: Re-imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation', *Risk Management: An International Journal*, 7, 4, pp.23-41.

Gibson, S.D., 2004, 'Open Source Intelligence: An Intelligence Lifeline', *RUSI Journal*, 149, 1, pp.16-22.

Gibson, S.D., 1997, *The Last Mission Behind the Iron Curtain*, Stroud: Sutton, ISBN: 0-7509-1408-4.

Gibson, S.D., 2004, 'Risk Management: Where Safety and Security Diverge', *Journal of the International Society for Respiratory Protection*, 21, Spring-Summer, pp.40-48.

Gibson, S.D., 2003, 'The Case for 'Risk Awareness'', *Security Journal*, 16, 3, pp.55-64.

Gibson, S.D., 2006, 'Evaluating Intelligence as a Public Contrition', *International Journal of Intelligence and CounterIntelligence*, 19, 1, pp.189-193.

Giddens, A., 2002, *Runaway World: How Globalisation is Reshaping Our Lives*, London: Profile Books, ISBN: 1-86197-429-9.

Giddens, A., 1991, *Modernity and Self-Identity*, Cambridge: Polity Press, ISBN: 0-745-60932-5.

Gill, M., (Ed), 2003, *Managing Security: Crime at Work*, Leicester: Perpetuity Press, ISBN: 1-899287-65-5.

Gill, P., Phythian, M., 2006, *Intelligence in an Insecure World*, Cambridge: Polity Press, ISBN: 0-7456-3245-9.

Gilmour, D., 2003, 'How to Fix Knowledge Management', *Harvard Business Review*, pp.1-8.

Gladwell, M., 2001, *The Tipping Point: How Little Things Can Make a Big Difference*, (Second Edition), London: Abacus, ISBN: 0-349-11346-7.

Glaser, B.B., Strauss, A.L., 1967, *The Discovery of Grounded Theory*, Chicago: Aldine, ISBN: 0-202-30260-1.

Glasser Susan, B., 'Probing Galaxies of Data for Nuggets', *Washington Post*, 25 November 2005.

Goleman, D., 1996, *Emotional Intelligence: Why it can Matter More than IQ*, London: Bloomsbury, ISBN: 0-747-52830-6.

Goodman, M.A., 2003, '9/11: The Failure of Strategic Intelligence', *Intelligence and National Security*, 18, 4, pp.59-71.

Goodman, M., 2006, 'Studying and Teaching about Intelligence: The Approach in the United Kingdom', *Studies in Intelligence: Journal of the American Intelligence Professional*, 50, 2.

Goss, P., Director Central Intelligence, 2005, *Global Intelligence Challenges 2005: Meeting Long-Term Challenges with a Long-Term Strategy*, Senate Select Committee on Intelligence, Washington DC, on 16 February 2005.

Goss, P., 2004, 'DCI Goss Addresses Employees', available at: http://www.fas.org/irp/cia/product/goss092404.pdf

Graham, J. D., Wiener, J. B., (Ed), 1995, *Risk versus Risk: Tradeoffs in Protecting Health and the Environment*, Cambridge: Harvard University, ISBN: 0-674-77304-7.

Granger, M.M., 1993, 'Risk Analysis and Management', *Scientific American*, July 1993, pp.24-30.

Gray, C.S., 2005, *Another Bloody Century: Future Warfare*, London: Weidenfeld & Nicholson, ISBN: 0-297-84627-2.

Gray, J., 2003, *Al Qaeda and What it Means to be Modern*, London: Faber & Faber, ISBN: 0-571-21980-2.

Gray, J., 2002, *Straw Dogs: Thoughts on Humans and Other Animals*, London: Granta Books, ISBN: 1-86207-512-3.

Gray, J., 1998, *False Dawn: The Delusions of Global Capitalism*, London: Granta Books, ISBN: 1-86207-530-1.

Grayling, A.C., 2003, *Life, Sex and Ideas: The Good Life Without God*, Oxford: Oxford University Press, ISBN: 0-19-517755-X.

Greider, W., 2003, *The Soul of Capitalism: Opening Paths to a Moral Economy*, New York: Simon & Schuster, ISBN: 0-684-86219-0.

Grove-White, R., 2001, 'New Wine, Old Bottles? Personal Reflections on the New Biotechnology Commissions.', *The Political Quarterly Publishing Co. Ltd.*, 2001, 3, pp.466-472.

Gummesson, E., 2000, *Qualitative Methods in Management research*, London: Sage Publications, ISBN: 0-761-92014-5.

Gunaratna, R., 2002, *Inside Al Qae'da*, Hurst & Co, ISBN: 1-850-65671-1.

Haas, C.N., 2002, 'The Role of Risk Analysis in Understanding Bioterrorism', *Risk Analysis: An International Journal*, 22, 4, pp.671-677.

Habermas, J., Shapiro, J.J., (Eds), 1986, *Knowledge and Human Interests*, London: Polity Press, ISBN:0-745-60459-5.

Halevy, E., 2004, 'Intelligence and the Making of Foreign Policy: A Personal Reflection', 21 June 2004, The Portland Trust.

Hansen, J., 2004, 'US Intelligence Confronts the Future', *International Journal of Intelligence and CounterIntelligence*, 17, 4, pp.673-709.

Harvard Business School, (Ed), 1998, *Harvard Business Review on Knowledge Management*, Boston: Harvard Business School Publishing, ISBN: 0-87584-881-8.

Hassett, A., Sigal, L., 2002, 'Unforeseen Consequences of Terrorism: Medically Unexplained Symptoms in a Time of Fear', *Archives of Internal Medicine*, 162, 16, pp.1809-1813.

Hatfield, A.J., Hipel, K.W., 2002, 'Risk and Systems Theory', *Risk Analysis: An International Journal*, 22, 6, pp.1043-1057.

Hayes, S.F., 2006, *Post-Haste*, available at: http://www.weeklystandard.com/Content/Public/Articles/000/000/011/975brvct.asp

Healey, M., 2005, 'DiRDDy Bomb', *NBC International*, pp.24-25.

Hearnden, K., 1993, *The Management of Security in the UK: A Research Survey*, SITO & Loughborough University, Loughborough.

Hearndon, K., Moore, A., 1999, *The Handbook of Business Security: A Practical Guide to Managing the Security Risk*, (2nd Edition), London: Kogan Page, ISBN: 0-7494-2923-2.

Heartfield, J., 1996, The Limits of Social Construction Theory, in: *A Moral Impulse: The End of Capitalist Triumphalism*, Revell, L., Heartfield, James, 1996, (Eds.), London: Junius Publications, pp.47-89

Held, D., 2004, *Global Covenant*, London: Polity Press, ISBN: 0-745-63353-6.

Held, D., 1997, 'How to Rule the World', *New Statesman*, 29 August 1997, pp.28-31.

Held, D., McGrew, A., 2003, *Globalization/Anti-Globalization*, Malden, MA: Polity Press, ISBN: 0-7456-2989-X.

Held, D., McGrew, A., 2002, *Governing Globalization: Power, Authority and Global Governance*, Malden: Blackwell Publishing, ISBN: 0-7456-2733-1.

Hennessy, P., 2005, 'The British Secret State: Old and New', *RUSI Journal*, 150, 3, pp.16-22.

Hennessy, P., 2007 (Ed), *The New Protective State: Government, Intelligence and Terrorism*, London: Continuum Books, ISBN: 978-0-8264-9614-0.

Herman, M., 2004, 'Intelligence and the Iraqi Threat: British Joint Intelligence after Butler', *RUSI Journal*, August, pp.18-24.

Herman, M., 2003, 'Counter-Terrorism, Information Technology and Intelligence Change', *Intelligence and National Security*, 18, 4, pp.40-58.

Herman, M., 1999, 'Modern Intelligence Services: Have They a Place in Ethical Foreign Policies?', *Conflict Studies Research Centre*, M18, September 1999,

Herman, M., 2005, 'Getting Value out of Intelligence: A British Experience', 29 August 2005, Intelligence Consumers Conference, Stockholm.

Herman, M., 1996, *Intelligence Power in Peace and War*, Cambridge: Royal Institute of International Affairs, ISBN: 0-521-56636-3.

Herman, M., 2001, *Intelligence Services in the Information Age*, London: Frank Cass, ISBN: 0-7146-196-2.

Herman, M., McDonald, J.K., Masny, V., 2006, *Did Intelligence Matter in the Cold War?*, Oslo: Institutt for Forsvarsstudier (Norwegian Institute for Defence Studies), ISBN: 0333-3981.

Hillson, D., (Ed), 2006, *The Risk Management Universe*, London: British Standards Institution, ISBN: 0-580-43777-9.

Hillson, D., Murray-Webster, Ruth., 2005, *Understanding and Managing Risk Attitude*, Aldershot: Gower Publishing, ISBN: 0-566-08627-1.

Hitz, F.P., 2000, 'The Future of American Espionage', *International Journal of Intelligence and CounterIntelligence*, 13, 1, pp.1-20.

Hoffman, B., 2001, *Re-Thinking Terrorism in Light of a War on Terrorism*, Subcommittee on Terrorism and Homeland Security House Permanent Select Committee on Intelligence, 26 September 2001.

Holden-Rhodes, J.F., 1997, *Sharing the Secrets: Open Source Intelligence and the War on Drugs*, West Port, CT: Praeger, ISBN: 0-275-95454-4.

Holmes, A., 2004, *Smart Risk*, Chichester: Capstone Publishing Limited, ISBN: 1-84112-507-5.

Honoré, C., 2004, *In Praise of Slow: How a World-Wide Movement is Challenging the Cult of Speed*, London: Orion Books, ISBN: 0-75285-625-1.

Hood, C., Heald, D., 2006, *Transparency: The Key to Better Governance?*, Oxford: Oxford University Press, ISBN: 978-0-19-726383-9.

Hough, P., 2004, *Understanding Global Security*, Abingdon: Routledge, ISBN: 0-415-29666-8.

Howard, M., 2002, *Clausewitz: A Very Short Introduction*, Oxford: Oxford University Press, ISBN: 0-19-280257-7.

Hughes-Wilson, J., 2004, *Military Intelligence Blunders and Cover-ups*, (Revised Edition), London: Robinson, ISBN: 1-84119-871-4.

Hulnick, A.S., 1999, 'Openness: Being Public About Secret Intelligence', *International Journal of Intelligence and CounterIntelligence*, 12, 4, pp.463-483.

Hulnick, A.S., 2001, 'Dirty Tricks for Profit: Covert Action in Private Industry', *International Journal of Intelligence and CounterIntelligence*, 14, 4, pp.529-544.

Hulnick, A.S., 2002, 'The Downside of Open Source Intelligence', *International Journal of Intelligence and CounterIntelligence*, 15, 4, pp.565-579.

Hulnick, A.S., 1999, *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Westport: Praeger, ISBN: 0-275-96653-4.

Hulnick, A.S., 2005, 'Does the US Intelligence Community Need a DNI?', *International Journal of Intelligence and CounterIntelligence*, 17, 4, pp.710-730.

Hulnick, A.S., 2004, *Keeping Us Safe: Secret Intelligence and Homeland Security*, Westport, CT: Praeger, ISBN: 0-275-98150-9.

Hulnick, A.S., 2006, 'US Intelligence Reform: Problems and Prospects', *International Journal of Intelligence and CounterIntelligence*, 19, 3, pp.302-315.

Hulnick, A.S., 2006, 'What's Wrong with the Intelligence Cycle', *Intelligence and National Security*, 21, 6, pp.959-979.

Hume, M., 2005, *The Age of Intolerant Tolerance*, available at: www.spiked-online.com/Printable/0000000CAD0A.tm

Hunt, B., 2004, *The Timid Corporation: Why Business is terrified of Taking Risk*, London: Wiley, ISBN: 0-470-84368-3.

Huntington, S.P., 2002, *The Clash of Civilizations and the Re-making of World Order*, London: Simon & Schuster, ISBN: 0-7432-3149-X.

Hussey, J., Hussy, R., 1997, *Business Research: A Practical Guide for Undergraduate and Postgraduate Students*, London: Macmillan Press, ISBN: 0-333-60705-8.

Hutton, B., 2004, *Report of the Inquiry into the Circumstances Surrounding the Death of Dr David Kelly CMG*, House of Commons, Westminster, Report No: HC 247.

Hyams, K.C., Murphy, F.M., Wessely, S., 2002, '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*, 27, 2, pp.273-291.

Jacoby, L.E., Defense Intelligence Agency, 2005, *Current and Projected National Security Threats to the United States*, Senate Select Committee on Intelligence, Washington DC, 16 February 2005.

Jaeger, C.C., Renn, O., Rosa, E.A., Webler, T., 2001, *Risk, Uncertainty, and rational Action.*, London: Earthscan, ISBN: 185383-770-9.

James, O., 2007, *Affluenza*, London: Vermilion, ISBN: 978-0-09-190010-6.

Jardines, E.A., 2005, *Written Testimony: Using Open-Source Information Effectively*, The House Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment, Washington, 21 June 2005.

Jeffreys-Jones, R., 2003, *Cloak and Dollar: A History of American Secret Intelligence*, (Second Edition), London: Yale University Press, ISBN: 0-300-10159-7.

Jeffson, J., 2005, 'Creating an Open Source Capability', *Military Intelligence Professional Bulletin*, October-December 2005, pp.40-44.

Johnson, L.K, 2000, 'The DCI vs the Eight-Hundred-Pound Gorilla', *International Journal of Intelligence and CounterIntelligence*, 13, 1, pp.35-48.

Johnson, L.K., 2003, 'Bricks and Mortar for a Theory of Intelligence', *Comparative Strategy*, 22, 1, pp.1-28.

Johnson, L.K., 2003, 'Preface to a Theory of Strategic Intelligence', *International Journal of Intelligence and CounterIntelligence*, 16, pp.638-663.

Johnson, L.K., 2002, *Bombs, Bugs, Drugs, and Thugs*, New York: New York University Press, ISBN: 0-8147-4253-X.

Johnson, L.K., 1990, 'The Role of Congress in US Strategic Intelligence', *American Intelligence Journal*, Summer/Fall, pp.41-45.

Johnston, R., 2003, 'Foundations for Meta-Analysis: Developing a Taxonomy of Intelligence Analysis Variables', *Studies in Intelligence: Journal of the American Intelligence Professional*, 47, 3.

Johnston, R., 2005, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, Washington DC: Center for the Study of Intelligence, Central Intelligence Agency, ISBN: 1-929667-13-2.

Jones, C., 2006, "Where the State Feared to Tread': Britain, Britons, Covert Action and the Yemen Civil War, 1962-64', *Intelligence and National Security*, 21, 5, pp.717-737.

Joy, B., 2000, 'Why the Future Doesn't Need Us', *Wired Magazine*, 1 April 2000,

Kagan, R., 2003, *Paradise and Power: America and Europe in the New World Order*, London: Atlantic Books, ISBN: 1-84354-177-7.

Kasperson, J.X., Kasperson, R.E., 2005, *The Social Contours of Risk Volume 1: Publics, Risk Communication & the Social Amplification of Risk*, London: Earthscan, ISBN: 1-84407-073-5.

Kasperson, J.X., Kasperson, R.E., 2005, *The Social Contours of Risk Volume 2: Risk Analysis, Corporations and the Globalisation of Risk*, London: Earthscan, ISBN: 1-84407-175-8.

Keegan, J., 2003, *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, (Pimlico Edition 2004 Edition), London: Pimlico, ISBN: 0-7126-6650-8.

Kent, S., 1966, *Strategic Intelligence for American World Policy*, Princeton, NJ: Princeton University, ISBN: 0-691-02160-0.

Keohane, R., 1998, 'International Institutions: Can Interdependence Work?', *Foreign Policy*, Spring, 110, pp.82-97.

Kim, C.W., Mauborgne, R., 2003, 'Tipping Point Leadership', *Harvard Business Review*, April 2003, pp.60-69.

Kindsvater, L.C., 2003, 'The Need to Reorganize the Intelligence Community', *Studies in Intelligence: Journal of the American Intelligence Professional*, 47, 1.

King, D.A., 2004, 'The Scientific Impact of Nations: What Different Countries Get for Their Research Spending', *Nature*, 430, July, pp.311-316.

King, N., 2003, 'The Influence of Anxiety: September 11, Bioterrorism, and American Public Health', *Journal of Historical Medicine*, 58, pp.433-441.

Kinsey, C., 2005, 'Regulation and Control of Private Military Companies: The Legislative Dimension', *Contemporary Security Policy*, 26, 1, pp.84-102.

Kissenger, H., 1994, *Diplomacy*, London: Simon & Schuster, ISBN: 0-671-51099-1.

Klein, N., 2000, *No Logo*, London: Flamingo, ISBN: 0-00-653040-0.

Klinke, A., Renn, O., 2002, 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies', *Risk Analysis: An International Journal*, 22, 6, pp.1071-1094.

Knight, D.W., 2001, 'The Fourth Wish: Operational Information Management and Situational Awareness', *Canadian Military Journal*, Winter, pp.33-40.

Knightley, P., 2003, *The Second Oldest Profession: Spies and Spying in the Twentieth Century*, (Second Edition), London: Pimlico, ISBN: 1-8441-3091-6.

Krimsky, S., Golding, D., (Eds), 1992, *Social Theories of Risk*, Westport: Praeger, ISBN:0-275-94317-8.

Krizan, L., 1999, *Intelligence Essentials for Everyone*, (Number 6 Edition), US Joint Military Intelligence College, Washington DC.

Kunreuther, H., 2002, 'Risk Analysis and Risk Management in an Uncertain World', *Risk Analysis: An International Journal*, 22, 4, pp.655-664.

Kunreuther, H., 2002, 'The Role of Insurance in Managing Extreme Events: Implications for Terrorism Coverage', *Risk Analysis: An International Journal*, 22, 3, pp.427-437.

Lahneman, W.J., 2004, 'Knowledge-Sharing in the Intelligence Community After 9/11', *International Journal of Intelligence and CounterIntelligence*, 17, 4, pp.614-633.

Lahneman, W.J., 2007, 'Is a Revolution in Intelligence Affairs Occurring?', *International Journal of Intelligence and CounterIntelligence*, 20, 1, pp.1-17.

Lahnemann, W.J., 2003, 'Outsourcing the IC's Stovepipes', *International Journal of Intelligence and CounterIntelligence*, 16, pp.573-593.

Laqueur, W., 1985, *A World of Secrets: The Uses and Limits of Intelligence*, New York: Basic Books, ISBN: 1-560-00594-7.

Lash, S., Szerszynski, B., Wynne, B., (Ed), 1996, *Risk, Environment & Modernity: Towards a New Ecology*, London: Sage, ISBN: 0-8039-7938-X.

Lawrence, F., 2004, *Not on the Label: What Really Goes into the Food on your Plate*, London: Penguin, ISBN: 0-141-01566-7.

Levine, R., Locke, C., Searls, Doc., Weinberger, D., 2000, *The Cluetrain Manifesto: The End of Business as Usual*, Cambridge, MA: Perseus Books Group, ISBN: 0-7382-0431-5.

Levitt, S.D., Dubner, S.J., 2005, *Freakonomics*, London: Penguin Books, ISBN: 0-141-01901-8.

Lewis, B., 2004, *The Crisis of Islam: Holy War and Unholy Terror*, Phoenix, ISBN: 0-75381-752-7.

Lind, M., 2003, *Made in Texas: George W. Bush and the Southern Takeover of American Politics*, New York: Basic Books, ISBN: 0-456-04121-3.

Lomborg, B., 2001, *The Skeptical Environmentalist: Measuring the Real State of the World*, Cambridge: Cambridge University Press, ISBN: 0-521-01068-3.

Losey, S., 2006, *Top Intel Analyst Focuses on Work Force, Data Sharing*, available at: http://federaltimes.com/index.php?S=1480846

Lovelock, J., 2000, *The Ages of Gaia: A Biography of Our Living Earth*, Oxford: Oxford University Press, ISBN: 0-19-286217-0.

Lowenthal, M.M., 1999, 'Open Source Intelligence: New Myths, New Realities', *Intelligencer*, 10, 1, pp.7-9.

Lowenthal, M.M., 2003, *Intelligence: From Secrets to Policy*, Washington: CQ Press, ISBN: 1-56802-759-1.

Löfstedt, R.E., Fischhoff, B., Fischhoff, I.R., 2002, 'Precautionary Principles: General Definitions and Specific Applications to Genetically Modified Organisms', *Journal of Policy Analysis and Management*, 21, 3, pp.381-407.

Madill, D.L., 2005, 'Producing Intelligence from Open Sources', *Military Intelligence Professional Bulletin*, October-December 2005, pp.19-26.

Malik, K., Gee, M., Levitt, N., O'Hear, A., Ridley, M., Ryan, K., Wrawick, K., 2001, *What is it to be Human? What Science Can and Cannot Tell Us*, London: Academy of Ideas, ISBN: 1-904025-00-5.

Mannunta, G., 2002, 'Risk and Security: Are They Compatible Concepts', *Security Journal*, 15, pp.43-55.

Manunta, G., 1998, *Security: An Introduction*, Cranfield University, ISBN: 1-8713-15-68-9.

Markowitz, J., 2003, 'Open Source: In Support of All-Source Intelligence', *Open Source Solutions 2003*, Washington DC, USA, September 2003.

Marrin, S., 2007, 'At Arm's Length or at the Elbow?: Explaining the Distance between Analysts and Decisionmakers', *International Journal of Intelligence and CounterIntelligence*, 20, 3, pp.401-414.

Marrin, S., Clemente, J., 2006, 'Modeling an Intelligence Analysis Profession on Medicine', *International Journal of Intelligence and CounterIntelligence*, 19, 4, pp.642-665.

Masse, T., Cumming, A., 2005, *Intelligence Reform Implementation at the Federal Bureau of Investigation: Issues and Options for Congress*, Library of Congress: Congressional Research Service, Washington, Report No: RL33033, available at: http://www.fas.org/sgp/crs/intel/RL33033.pdf

Mathieu, F., Dearden, N., 2006, *Corporate Mercenaries: The Threat of Private Military and Security Companies*, War on Want, London, available at: http://www.waronwant.org/Corporate+Mercenaries+13275.twl

Maybury, M.T., 1998, *Tools for the Knowledge Analyst: An Information Superiority Visionary Demonstration*, The Mitre Corporation Advanced Information Systems Center, available at: http://plato.acadiau.ca/courses/comp/tomek/Collaboration%20over%20Internet/CVW/Documents/Tools%20for%20the%20Knowledge%20Analyst.htm

McCutcheon, D.M., Meredith, J.R., 1993, 'Conducting Case Study Research in Operations Management', *Journal of Operations Management*, 11, pp.239-256.

McGee, A., 2007, *Corporate Security's Professional Project: An Examination of the Modern Condition of Corporate Security Management and the Potential for Further Professionalisation of the Occupation*, MSc Dissertation in the department of Defence Management and Security Analysis, Cranfield University.

McIntyre, S.G., Gauvin, M., Waruszynski, B., 2003, 'Knowledge Management in the Military Context', *Canadian Military Journal*, Spring, pp.35-40.

Medina, C.A., 2002, 'The Coming Revolution in Intelligence Analysis: What to Do When Traditional Models Fail', *Studies in Intelligence: Journal of the American Intelligence Professional*, 46, 3.

Mercado, S., 2004, 'A Venerable Source in a New Era: Sailing the Sea of OSINT in the Information Age', *Studies in Intelligence: Journal of the American Intelligence Professional*, 48, 3.

Mercado, S.C., 2005, 'Reexamining the Distinction Between Open Information and Secrets', *Studies in Intelligence: Journal of the American Intelligence Professional*, 49, 2.

Mercado, S.C., 2001, 'Open Source Intelligence from the Airwaves: FBIS Against the Axis, 1941-1945', *Studies in Intelligence: Journal of the American Intelligence Professional*, Fall-Winter, 11.

Meyer, H.E., 2004, *Connecting the Dots: Our Intelligence Community Needs Patter-Spotters, not Career Bureaucrats*, Athens, Research Institute for European and American Studies,

Miles, M., Huberman, M., 1994, *Qualitative Data Analysis: An Expanded Sourcebook*, (Second Edition), London: Sage Publications, ISBN: 0-8039-5540-5.

Mill, J.S., 1974, *On Liberty*, London: Penguin Classics, ISBN: 0-14-043207-8.

Mirza, M., Senthilkumaran, A., Ja'far, Z., Report No: 241, 2007, *Living Apart Together: British Muslims and the Paradox of Multiculturalism*, Policy Exchange, London, available at: http://www.policyexchange.org.uk/images/libimages/241.pdf

Miscik, J.A., 2004, *DDI's State of Analysis Speech*, available at: http://www.fas.org/irp/cia/product/021104miscik.pdf

MITRE Corporation, Report No: JSR-04-132, 2004, *Horizontal Integration: Broader Access Models for Realizing Information Dominance*, JASON Program Office.

Mitroff, I.I., Alpaslan, M.C., 2003, 'Preparing for Evil', *Harvard Business Review*, April 2003, pp.109-115.

Mongoven, B., 2005, *The Evolution of Market Campaigns*, e-mail subscription dated 29 September 05.

Moore, D.T., Krizan, L., Moore, E.J., 2005, 'Evaluating Intelligence: A Competency-Based Model', *International Journal of Intelligence and CounterIntelligence*, 18, 2, pp.204-220.

Moore, M., 2002, *Stupid White Men*, (Second Edition), London: Penguin Books, ISBN: 0-141-01190-4.

Morgan, G., Smircich, L., 1980, 'The Case of Qualitative Research', *Academy of management Review*, 5, pp.491-500.

Morris, J., Bate, R., (Eds), 1999, *Fearing Food: Risk, Health & Environment*, Oxford: Butterworth Heinemann, ISBN: 0-7506-4222-X.

Morse, J., (Ed), 1993, *Critical Issues in Qualitative Research Methods*, Thousand Oaks, CA: Sage Publications, ISBN: 0-803-95043-8.

Mueller, R.S.I., Federal Bureau of Investigation, 2005, *Current and Projected National Security Threats to the United States*, Senate Select Committee on Intelligence, Washington DC, 16 February 2005.

Mulgan, G., Steinberg, T., Salem, O., 2005, *Wide Open: Open Source Methods and Their Future Potential*, London: DEMOS, ISBN: 1-84180-142-9.

Musser, G., 2005, 'The Climax of Humanity', *Scientific American*, 22 August 2005.

Mythen, G., 2004, *Ulrich Beck: A Critical Introduction to the Risk Society*, London: Pluto Press, ISBN: 0-7453-1814-2.

Nalla, M., Morash, M., 2002, 'Assessing the Scope of Corporate Security: Common Practices and Relationships with Other Business Functions', *Security Journal*, 15, 3, pp.7-19.

Netherlands General Intelligence and Security Service (AIVD), 2005, *Annual Report 2004*, The Hague, available at: https://www.aivd.nl/

Neumann, P.R., Smith M.L.R., 2005, 'Missing the Plot: Intelligence and Discourse Failure', *Orbis*, 2005, Winter, pp.95-107.

Newman, V., 2002, *The Knowledge Activist's Handbook*, Oxford: Capstone, ISBN: 1-84112-320-X.

Nicholson, N., 2001, *A Guide to Executive Protection*, Leicester: Perpetuity Press, ISBN: 1-899287-59-0.

Nitecki, D., Franklin, B., 1999, 'New Measures for Research Libraries', *The Journal of Academic Librarianship*, 25, 6, pp.484-487.

Nomikos, J.M., 2004, *Intelligence Requirements for Peacekeeping Operations*, Athens, Research Institute for European and American Studies.

Nonaka, I., Takeuchi, H., 1995, *The Knowledge-Creating Company*, Oxford: Oxford University Press, ISBN: 0-19-509269-4.

Nye, J.S., Jr., 2004, *Soft Power: The Means to Success in World Politics*, Cambridge MA: Public Affairs, ISBN: 1-58648-225-4.

O'Hara, K., 2004, *Trust: From Socrates to Spin*, Cambridge: Icon Books, ISBN: 1-84046-531-X.

O'Neill, B., 2006, *Waaah, it's all Blair's Fault*, available at: http://www.spiked-online.com/index.php?/site/article/1481/

O'Neill, O., 2002, *A Question of Trust: The BBC Reith Lectures 2002*, Cambridge: Cambridge University Press, ISBN: 0-521-52996-4.

Odom, W., 2003, *Fixing Intelligence for a more Secure America*, New Haven: Yale, ISBN: 0-300-09976-2.

Oliver, J., 2003, *They F*** You Up*, London: Bloomsbury, ISBN: 0-747-5677-X.

Ormerod, P., 2005, *Why Most Things Fail: Evolution, Extinction and Economics*, London: Faber and Faber, ISBN: 0-571-22012-6.

Oxford Analytica, 2006, *Spies, Lies & Intelligence: A Briefing Book prepared by Oxford Analytica*, Oxford Analytica, Oxford.

Palmer, M., 2003, *Breaking the Real Axis of Evil*, Oxford: Rowman & Littlefield, ISBN: 0-7425-3254-2.

Pappas, A.A., Simon, J.M.Jr., 2002, 'Daunting Challenges, Hard Decisions: The Intelligence Community: 2001-2015', *Studies in Intelligence: Journal of the American Intelligence Professional*, 46, 1.

Peak, D., 2005, 'DOD and the DNI Open Source Center - Building the Partnership', *Military Intelligence Professional Bulletin*, October-December 2005, pp.18-19.

Perl, R., 2005, *Combating Terrorism: The Challenge of Measuring Effectiveness*, Congressional Research Service: The Library of Congress, Washington, Report No: RL33160.

Perrow, C., 1999, *Normal Accidents: Living with High-Risk Technologies*, Chichester: Princeton University Press, ISBN: 0-691-00412-9.

Perry-Barlow, J., 2002, 'Why Spy?', *Forbes*, 10th July 2002.

Peterson, M., 1999, 'Critical Thinking: Analysis at its Best', *Intersec*, February, pp.36-39.

Peterson, P.G., 2004, *Running on Empty*, New York: Farrar, Straus & Giroux, ISBN: 0-374-25287-4.

Petro, J.B., 2004, 'Intelligence Support to the Life Science Community: Mitigating Threats from Bioterrorism', *Studies in Intelligence: Journal of the American Intelligence Professional*, 48, 3.

Petterson, J.S., 1988, 'Perception vs. Reality of Radiological Impact: The Goiânia Model', *Nuclear News*, 31, 14, pp.84-90.

Pew Internet and American Life Project, 2005, *The Future of the Internet*, Washington, available at: http://www.pewinternet.org/PPF/r/145/report_display.asp

Pham, T.N., 2003, *Open Source Intelligence: Doctrine's Neglected Child*, Newport, (R.I.): US Naval War College.

Phillips, E.M., Pugh, D.S., 2001, *How to Get a PhD*, (Third Edition), Buckingham: Open University Press, ISBN: 0-335-20550-X.

Pickford, J., (Ed), 2001, *Mastering Risks*, London: Pearson Education, ISBN: 0-273-65379-2.

Pidgeon, N.F., 1991, 'Safety Culture and Risk Management Organisations', *Journal of Cross-Cultural Psychology*, 22, 1, pp.129-140.

Pidgeon, N., Kasperson, R.E., Slovic, P., (Eds), 2003, *The Social Amplification of Risk*, Cambridge: Cambridge University Press, ISBN:0-521-52044-4.

Pilger, J., 2002, *The New Rulers of the World*, London: Verso, ISBN: 1-85984-412-X.

Pither, C., 2005, *You Can't be too Careful, Can You*, available at: www.spiked-online.com/Printable/0000000CAD08.tm

Politi, A., 2003, 'The Citizen as "Intelligence Minuteman"', *International Journal of Intelligence and CounterIntelligence*, 16, pp.34-38.

Popper, K., 1935, *The Logic of Scientific Discovery*, Abingdon: Routledge, ISBN: 0-415-27844-9.

Popper, K., 1945, *The Open Society and its Enemies - Volume One: The Spell of Plato*, (1995 Edition), Abingdon: Routledge, ISBN: 0-415-23731-9.

Popper, K., 1945, *The Open Society and its Enemies - Volume Two: Hegel and Marx*, (1995 Edition), Abingdon: Routledge, ISBN: 0-415-27842-2.

Powell, J.H., 2002, 'Bringing Terrorism into the Strategic Debate: An Expanded Characterisation of Strategic Threats to Firms', *Security Journal*, 15, pp.21-35.

Power, M., 1994, *The Audit Explosion*, London: ISBN: 1-898309-30-2.

Power, M., 2004, *The Risk Management of Everything*, London: Demos, ISBN: 1-84180-127-5.

Power, M., 2007, *Organized Uncertainty: Designing a World of Risk Management*, Oxford: Oxford University Press, ISBN: 978-0-19-925394-4.

Prieto, D.B., Kirchhoff, C., 2005, 'Fits and Starts', *The Washington Times*, 25 August 2005.

Pringle, R.W., 2003, 'The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989', *International Journal of Intelligence and CounterIntelligence*, 16, pp.280-289.

Putnam, R., 2001, *Bowling Alone: The Collapse and Revival of American Community*, London: Simon & Schuster, ISBN: 0-743-20304-6.

RAND, 2006, *Towards a Theory of Intelligence*, RAND National Security Research Division & Office of DNI, Washington, Report No: 0-8330-3911-3.

Rathmell, A., 2002, 'Towards Postmodern Intelligence', *Intelligence and National Security*, 17, 3, pp.87-104.

Rawnsley, A., 2001, *Servants of the People: The Inside Story of New Labour*, (Revised Edition), London: Penguin Books, ISBN: 0-140-27850-8.

Rees, M., 2003, *Our Final Century: Will the Human Race Survive the Twenty-First Century*, London: William Heinemann, ISBN: 0-434-00809-5.

Rees, W., Aldrich, R., 2005, 'Contending Cultures of Counterterrorism: Transatlantic Divergence or Convergence?', *International Affairs*, 81, 5, pp.905-923.

Reese, D.A., 2005, '50 Years of Excellence: ASD Forges Ahead as the Army's Premier OSINT Unit in the Pacific', *Military Intelligence Professional Bulletin*, October-December 2005, pp.27-29.

Renier, O., Rubinstein, V., 1986, *Assigned to Listen: The Evesham Experience 1939-1943*, London: BBC Books, ISBN: 0-563-20508-3.

Renn, O., Klinke, A., 2002, 'A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies', *Risk Analysis: An International Journal*, 22, 6, pp.1071-1094.

Reynolds, G., 2006, *An Army of Davids: How Markets and Technology Empower Ordinary People to Beat Big Media, Big Government and Other Goliaths*, Nashville (TE): Nelson Current, ISBN: 1-5955-5054-2.

Rheingold, H., 2002, *Smart Mobs: The Next Social Revolution*, Cambridge, MA: Basic Books, ISBN: 0-7382-0861-2.

Richelson, J.T., 1999, '"Truth conquers all chains": The US Army Intelligence Support Activity, 1981 - 1989', *International Journal of Intelligence and CounterIntelligence*, 12, 2, pp.168-200.

Rischard, J.F., 2002, *High Noon: 20 Global Issues, 20 Years to Solve Them*, Oxford: Perseus Press, ISBN: 1-903985-49-8.

Rolington, A., 2006, 'Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11', *Intelligence and National Security*, 21, 5, pp.738-759.

Ross, C., 2007, *Independent Diplomat: Dispatches from an Unaccountable Elite*, London: Hurst & Company, ISBN: 978-1-85065-843-6.

Ross, J.F., 1999, *The Polar Bear Strategy: Reflections on Risk in Modern Life*, USA: Perseus Books, ISBN: 0-7382-0117-0.

Runciman, D., 2006, *The Politics of Good Intentions: History, Fear and Hypocrisy in the New World Order*, Woodstock: Princeton University Press, ISBN: 0-691-12566-X.

Rushkoff, D., 2003, *Open Source Democracy: How Online Communication is Changing Offline Politics*, London: DEMOS, ISBN: 1-84180-113-5.

Saatchi, M., 2006, *In Praise of Ideology*, Centre for Policy Studies, London, ISBN: 1-905-389-40-X.

SACLANT Intelligence Branch, 2001, *NATO Open Source Intelligence Handbook*, dated: November 2001.

SACLANT Intelligence Branch, 2002, *Intelligence Exploitation of the Internet*, dated: October 2002.

SACLANT Intelligence Branch, 2002, *NATO Open Source Intelligence Reader*, dated: February 2002, available at: http://www.au.af.mil/au/awc/awcgate/nato/osint_reader.pdf

Sagan, C., 1994, *Pale Blue Dot: A Vision of the Human Future in Space*, New York: Random House, ISBN: 0-679-76486-0.

Sapolosky, H., (Ed), 1986, *Consuming Fears: The Politics of Product Risks*, New York: Basic Books, ISBN:0-465-01411-9.

Sardar, Z., Wyn-Davies, M., 2002, *Why Do People Hate America?*, Cambridge: Icon Books, ISBN: 1-84046-525-5.

Schwartz, D. G., Divitni, M., Brasethvik, T., (Ed), 2000, *Internet-Based Organizational Memory and Knowledge Management*, Idea Group, ISBN:1-878-28982-9.

Schwing, R., 2002, 'A Mental Model Proposed to Address Sustainability and Terrorism Issues', *Risk Analysis: An International Journal*, 22, 3, pp.415-420.

Schwing, R. C., Albers, W. A. J., (Ed), 1980, *Societal Risk Assessment: How Safe is Safe Enough?*, New York: Plenum Press, ISBN:0-306-40554-7.

Scoble, R., Israel, S., 2006, *Naked Conversations: How Blogs are Changing the Way Businesses Talk with Customers*, Hoboken (NJ): John Wiley & Sons, ISBN: 0-471-74719-X.

Scott, L., Jackson, P., 2004, 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security*, 19, 2, pp.139-169.

Scott, L., Hughes, R.G., 2006, 'Intelligence, Crises and Security: Lessons from History?', *Intelligence and National Security*, 21, 5, pp.653-674.

Scruton, R., 2002, *The West and the Rest: Globalization and the Terrorist Threat*, London: Continuum, ISBN: 0-8264-7030-0.

Seaquist, L., 2004, 'Intelligence for Grownups', *Christian Science Monitor*, 6 December 2004.

Seifert, J.W., Report No: RL31798, 2006, *Data Mining and Homeland Security: An Overview*, Congressional Research Service: The Library of Congress, Washington, available at: http://www.fas.org/sgp/crs/intel/RL31798.pdf

Sellitz, C., Wrightsman, L.S., Cook, S.M., 1976, *Research Methods in Social Relations*, (3rd Edition), New York: Holt, Rinehart & Winston, ISBN: 0-030-80986-X.

Sharon, B., 2005, *Operational Risk Management: The Difference Between Risk Management and Compliance*, available at: http://www.continuitycentral.com/feature0243.htm

Shimell, P., 2002, *The Universe of Risk*, London: Pearson Education, ISBN: 0-273-65642-2.

Shorrock, T., 2005, *The Spy Who Billed Me*, available at: http://www.motherjones.com/news/outfront/2005/01/12_400.html

Shpiro, S., 2001, 'The Media Strategies of Intelligence Services', *International Journal of Intelligence and CounterIntelligence*, 14, 4, pp.485-502.

Shulsky, A.N., Schmitt, G J., 2002, *Silent Warfare: Understanding the World of Intelligence*, Dulles: Brassey's, Inc, ISBN: 1-574-88345-3.

Silberman, L.H., Robb, C.S., 2005, *US Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, Washington DC, Report No: 20503.

Silverman, D., 2004, *Interpreting Qualitative Data: Methods for Analysing Talk, Text and Interaction*, (2nd Edition), London: Sage, ISBN: 0-7619-6865-2.

Simonsen, C.E., Manunta, G., 1996, 'Is Security Management a Profession?', *International Journal of Risk, Security and Crime Prevention*, 1, 3, pp.229-240.

Sims, J. E., Gerber, B., (Eds), 2005, *Transforming US Intelligence*, Washington, DC.: Georgetown University Press, ISBN:1-58901-069-7.

Sirak, M., 2004, 'Interview with George Lotz', *Janes Defence Weekly*, 24 November 2004.

Sjöberg, L., 2002, 'Are Received Risk Perception Models Alive and Well?', *Risk Analysis: An International Journal*, 22, 4, pp.665-669.

Skolnik, M.L., 1998, 'Higher Education in the 21st Century', *Futures*, 30, 7, pp.635-650.

Slovic, P., 2000, *The Perception of Risk*, London: Earthscan, ISBN: 1-85383-528-5.

Slovic, P., 2002, 'Terrorism as Hazard: A New Species of Trouble', *Risk Analysis: An International Journal*, 22, 3, pp.425-426.

Slywotzky, A.J., Drzik, J., 2005, 'Countering the Biggest Risk of All', *Harvard Business Review*, April 2005, pp.88-98.

Smallman, C., 1996, 'Risk and Organizational Behaviour: A Research Model', *Disaster Prevention and Management*, 5, 2, pp.12-26.

Smith, J.K., 1983, 'Quantitative v. Qualitative Research: An Attempt to Clarify the Issue', *Educational Research*, March, pp.6-13.

Smith, M., 2003, *The Spying Game: The Secret History of British Espionage*, London: Politico's Publishing, ISBN: 1-84275-004-6.

Social Issues Research Centre, 2005, *Obesity and the Facts: An Analysis of Data from the Health Survey for England 2003*, Oxford.

Stake, R.E., 1995, *The Art of Case Study Research*, London: Sage Publications, ISBN: 0-8039-5767-X.

Star, C., 2003, 'The Precautionary Principle Versus Risk Analysis', *Risk Analysis: An International Journal*, 23, 1, pp.1-3.

Starr, S., 2005, *The Marks of Human Progress*, available at: www.spiked-online.com/Printable/0000000CAD09.tm

Starr, S., 2005, *The Virtual Library*, available at: http://www.spiked-online.com/Printable/0000000CAD73.htm

Steele R.D., 2006, *On Intelligence: Spies and Secrecy in an Open World*, Oakton (VA): OSS International Press, ISBN: 0-9715661-0-0.

Steele, R.D., 1996, 'Creating a Smart Nation: Strategy, Policy, Intelligence, and Information', *Government Information Quarterly*, 13, 2, pp.159-173.

Steele, R.D., 2002, Information Peacekeeping & the Future of Intelligence, 18th November 2002,

Steele, R.D., 2004, *Failure to Address Staff Findings on OSINT*, United Business Media,

Steele, R.D., 2002, *The New Craft of Intelligence Personal, Public, & Political*, Oakton (VA): OSS International Press, ISBN: 0-9715661-1-9.

Steele, R.D., 2001, *On Intelligence: Spies and Secrecy in an Open World*, Oakton (VA): OSS International Press, ISBN: 0-9715661-0-0.

Steele, R.D., 2000, 'Possible Presidential Intelligence Initiatives', *International Journal of Intelligence and CounterIntelligence*, 13, 4, pp.409-423.

Steele, R.D., 2002, 'Crafting Intelligence in the Aftermath of Disaster', *International Journal of Intelligence and CounterIntelligence*, 15, 2, pp.161-178.

Steele, R.D., 2004, *Intelligence and Democracy: A Commentary*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2004, *Representative Rob Simmons (R-CT-02) Obtains 417 House Votes in favour of OSINT as Essential Part of Reform Effort*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2004, *OSS CEO Reviews Lessons Learned form OSINT, GWOT and National Security Transformation - America at Risk*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2004, *GWOT, OSINT and Collective Intelligence Come Together at NYC Hackers Conference*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2004, *OSS.NET Applauds Recommendation for New OSINT Agency in 9/11 Commission Report*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2004, *Committee on the Present Nonsense Formed to Counter-Balance Committee on the Present Danger - US Losing its Mind at all Levels*, Oakton (VA), accessed at: http://www.oss.net

Steele, R.D., 2005, 'Intelligence Affairs: Evolution, Revolution, or Reactionary Collapse', *International Journal of Intelligence and CounterIntelligence*, 19, 1, pp.187-189.

Steele, R.D., 2004, 'Accessing the Full Range of Open Sources', *International Journal of Intelligence and CounterIntelligence*, 17, 1, p.183.

Steele, R.D., 2006, *Draft Chapter for Strategic Intelligence by Loch Johnson*, available at: http://www.oss.net/dynamaster/file_archive/060409/00b583e458c7fb78e96ddc3a8444ae30/STEELE%20Draft%20Chapter%20for%20Strategic%20Intelligence%20on%20OSINT%2c%202.4.doc on 2 December 2006.

Steele, R.D., 2004, *Public Intelligence Must Supersede Secret Intelligence*, accessed at: http://www.oss.net/extra/news/?module_instance=1&id=2370

Steele, R.D., 2006, *Draft Chapter for The Handbook of Intelligence Studies*, available at: http://www.oss.net/dynamaster/file_archive/060409/5432a5e19def62b82684a111fe03f899/STEELE%20OSINT%20FOR%20HANDBOOK%203.3%20Chapter.doc

Steele, R.D., Richelson, J.T., 2001, 'Too Broke to be Fixed', *International Journal of Intelligence and CounterIntelligence*, 14, 2, pp.297-298.

Stiglitz, J., 2002, *Globalization and its Discontents*, London: Penguin, ISBN: 0-141-01038-X.

Strauss, A., Corbin, J., 1998, *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (Second Edition), London: Sage Publications, ISBN: 0-8039-5940-0.

Tzu, S., 1994, *Art of War*, Oxford: Westview Press, ISBN: 0-8133-1951-X.

Sunstein, C.R., 2005, *Laws of Fear: Beyond the Precautionary Principle*, Cambridge: Cambridge University Press, ISBN: 0-521-61512-7.

Surowiecki, J., 2004, *The Wisdom of Crowds*, London: Little Brown, ISBN: 0-349-11605-9.

Sutcliffe, K.M., Weber, K., 2003, 'The high cost of accurate knowledge', *Harvard Business Review*, May, pp.74-82.

Taleb, N.N., 2004, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, London: Penguin Books. ISBN: 978-0-141-03148-4.

Taleb, N.N., 2007, *The Black Swan: The Impact of the Highly Improbable*, London: Penguin Books, ISBN: 978-0-713-99995-2.

Tallis, R., 'You Can be a Beast, but I'm Human', *The Times Online*, 29 October 2005.

Tallis, R., 2004, *Hippocratic Oaths: Medicine and its Discontents*, London: Atlantic Books, ISBN: 1-84354-127-0.

Tanji, M., 2006, *An Army of Analysts*, available at: http://www.weeklystandard.com/Content/Public/Articles/000/000/011/971dyipm.asp?pg=1

Taylor, M.C., 2005, 'Open Source Intelligence Doctrine', *Military Intelligence Professional Bulletin*, October-December 2005, pp.12-14.

Tenet, G.J., 2000, 'The CIA and the Security Challenges of the New Century', *International Journal of Intelligence and CounterIntelligence*, 13, 2, pp.133-143.

The Pew Research Center, 2002, *What The World Thinks in 2002*, The Albright Foundation (Madeleine Albright), Washington.

The Royal Society, 1992, *Risk: Analysis, Perception and Management*, The Royal Society, London, ISBN: 0-85403-467-6.

The Surveillance Studies Network, 2006, *A Report on the Surveillance Society*, The Information Commissioner, London, available at: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/02_11_06_surveillance.pdf

The Worldwatch Institute, 2004, *State of The World 2004: The Consumer Society*, The Worldwatch Institute, Washington.

Thomas, S.T., 2000, 'Hidden in Plain Sight: Searching for the CIA's "New Missions"', *International Journal of Intelligence and CounterIntelligence*, 13, 2, pp.144-159.

Thomas, S.T., 1988, 'Assessing Current Intelligence Studies', *International Journal of Intelligence and CounterIntelligence*, 2, 2, p.239.

Thompson, B.G., 2006, *Beyond Connecting the Dots: A VITAL Framework for Sharing Law Enforcement Intelligence Information*, US House Committee on Homeland Security Democratic Staff, Washington.

Thompson, C., 'Open-Source Spying', *New York Times*, 3 December 2006.

Thornburgh, N., 2005, 'The Invasion of the Chinese Cyberspies (and the Man Who Tried to Stop Them)', *Time*, 29 August 2005.

Transparency International, 2003, *Global Corruption Report 2003: Access to Information*, London: Profile Books, ISBN: 1-86197-476-0.

Treverton, G.F., 2003, 'Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons', *Intelligence and National Security*, 18, 4, pp.121-140.

Treverton, G.F., 2003, *Reshaping National Intelligence for an Age of Information*, Cambridge: Cambridge University Press, ISBN: 0-521-53349-X.

Trim, P.R., 2000, 'The Company Intelligence Interface and National Security', *International Journal of Intelligence and CounterIntelligence*, 13, 2, pp.204-214.

Tsuruoka, D., 'Getting Ready for Future Shocks', *Investor's Business Daily*, 3 February 2006.

Turner, M.A., 2005, *Why Secret Intelligence Fails*, Dulles (VA): Potomac Books, ISBN: 1-57488-890-0.

Turner, S., 2001, 'Intelligence for a New World Order', *Foreign Affairs*, pp.150-166.

Tussing, B.B., 2003, *Sharing Information for Homeland Security: Overcoming Obstacles of Technology, Process and Culture*, unpublished paper.

UK Civil Contingencies Secretariat, 2003, *Overview of Horizon Scanning Methods*, London: Civil Contingencies Secretariat.

UK HM Treasury, Report No: Cm 6238, 2004, *2004 Spending Review: Public Service Agreements 2005-2008*, HM Treasury, London: HMSO.

UK Intelligence & Security Committee, 2005, Report No: Cm 6510, *Annual Report 2004-2005*, London: HMSO.

UK Intelligence and Security Committee, 2004, Report No: Cm 6240, *Annual Report 2003-2004*, London: HMSO.

UK Intelligence and Security Committee, 2003, Report No: Cm 5837, *Annual Report 2002-2003*, London: HMSO.

UK Intelligence and Security Committee, 2002, Report No: Cm 5724, *Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombing on Bali 12 October 2002*, London: HMSO.

UK Intelligence and Security Committee, 2003, Report No: Cm 5972, *Iraqi Weapons of Mass Destruction - Intelligence and Assessments*, London: HMSO.

UK Intelligence and Security Committee, 2006, Report No: Cm 6864, *Annual Report 2005-2006*, London: HMSO.

UK Privy Councellors, 2004, Report No: HC 898, *Review of Intelligence on Weapons of Mass Destruction (The Butler Review)*, House of Commons, London: HMSO.

Umphress, D.A., 2005, 'Diving the Digital Dumpster', *Air and Space Power Journal*, XIX, 2005, pp.82-91.

Unsinger, P.C., 1999, 'Meeting a Commercial Need: The International Maritime Bureau', *International Journal of Intelligence and CounterIntelligence*, 12, 1, pp.58-72.

US Army, 2004, *US Army Field Manual - Intelligence 2-0*.

US Attorney General, 2003, *Memorandum of Understanding Between Intelligence Community, Federal Law Enforcement Agencies, and the Department of Homeland Security Concerning Information Sharing*, dated 4 March 2003, available at: http://www.fas.org/sgp/othergov/mou-infoshare.pdf

US Commission on the Roles and Capabilities of the United States Intelligence Community (Aspin-Brown Commission), 1996, *Preparing for the 21st Century: An Appraisal of US Intelligence*, Washington, DC: US Government Printing Office, available at: http://www.access.gpo.gov/intelligence/int/pdf/int003.pdf

US Congressional Research Service, Report No: RL33742, 2006, *9/11 Commission Recommendations: Implementation Status*, Congressional Research Service, Washington, available at: http://www.fas.org/sgp/crs/homesec/RL33742.pdf

US Department of Defense Joint Chiefs of Staff, 2004, *Joint and National Intelligence Support to Military Operations*, US DoD, ISBN: JP 2-01, available at: http://www.fas.org/irp/doddir/dod/jp2_01.pdf

US Department of Defense, 2004, *Dictionary of Military and Associated Terms - JP 1-02*.

US Department of Defense, 2005, *Section 1206 Public Law 108-375*, Pentagon, Washington, available at: http://www.fas.org/irp/agency/dod/1206report.pdf

US Department of Energy, 2003, *Twelfth Report on Inadvertent Release of Restricted Data and Formerly Restricted Data under Executive Order 12958 (U)*, US Department of Energy, Germantown.

US Headquarters Department of the Army, 2006, *Open Source Intelligence (FMI 2-22.9)*, dated: 5 December 2006, Washington, US DOD, available at: http://www.fas.org/irp/doddir/army/fmi2-22-9.pdf

US House of Representatives, 2005, *Sec. 931. Department of Defense Strategy for Open-Source Intelligence*, available at: http://www.fas.org/irp/congress/2005_cr/dod-osint.html

US House Permanent Select Committee on Intelligence, 1996, *IC 21: The Intelligence Community in the 21st Century*, Washington DC.

US Information Security Oversight Office, 2004, *Report on Cost Estimates for Security Classification Activities for 2004*, available at: http://www.fas.org/sgp/isoo/2004costs.pdf

US Joint Military Intelligence Training Center, 1996, *Open Source Intelligence: Professional Handbook*, dated October 1996,

US National Commission on Terrorist Attacks upon the United States, 2004, *The 9/11 Commission Report*, Washington: WW Norton & Company, ISBN: 0-393-32671-3.

US National Counterterrorism Center, 2005, *A Chronology of Significant International Terrorism for 2004*, US State Department, Washington.

US National Counterterrorism Center, 2004, *Chronology of Non-Significant International Terrorist Incidents, 2003 (Revised 6/22/04)*, US State Department, Washington.

US National Intelligence Council, 2000, *Global Trends 2015: A Dialogue About the Future With Nongovernment Experts*, US National Foreign Intelligence Board under direction of the DCI, Report No: NIC 2000-02.

US National Intelligence Council, 2004, *Mapping the Global Future: Report of the National Intelligence Council's 2020 Project*, US National Intelligence Council, Washington, available at: http://www.dni.gov/nic/NIC_2020_project.html

US Office of the Director of National Intelligence, Annex to the US National Intelligence Report, 2006, *The US Intelligence Community's Five Year Strategic Human Capital Plan*, US DNI, Washington.

US Office of the Director of National Intelligence, 2006, *Intelligence Community Directive 301: National Open Source Enterprise*, dated: 11 July 2007, Washington, DC., DNI, available at: http://www.dni.gov/electronic_reading_room/ICD301.pdf

US Office of the National Counterintelligence Executive (NCIX), 2005, *The National Counterintelligence Strategy of the United States*, NCIX, Washington, Report No: 2005-10007.

US Presidential Executive Order, Report No: 133888, 2005, *Further Strengthening the Sharing of Terrorism Information to Protect Americans*, available at: http://www.fas.org/irp/offdocs/eo/eo-13388.htm

US Senate Committee on Governmental Affairs, 2004, *Summary of Intelligence Reform and Terrorism Prevention Act of 2004*, US Senate, Washington, available at: http://www.fas.org/irp/congress/2004_rpt/s2845-summ.pdf

US Senate Governmental Affairs Committee, 2004, *Building an Agile Intelligence Community*, US Senate Governmental Affairs Committee, 8 September 2004.

USA Today, 2004, 'CIA Invests in Tech Start-Ups', *USA Today*, 3rd March 2004,

Van Maanen, J., 1979, 'Reclaiming Qualitative Methods for Organizational Research: A Preface', *ASQ*, pp.520-526.

Vickers, R.D. Jr., 2005, 'Intelligence Reform: Problems and Prospects', *Breakthroughs*, 14, 1, pp.3-21.

Vickers, R.D. Jr., 2006, 'The Intelligence Reform Quandary', *International Journal of Intelligence and CounterIntelligence*, 19, 3, pp.356-364.

Ward, S.R., 2002, 'Evolution Beats Revolution in Analysis', *Studies in Intelligence: Journal of the American Intelligence Professional*, 46, 3.

Ware, J., 2004, *What Will Lord Butler Say?*, available at: http://news.bbc.co.uk/1/low/programmes/panorama/3883703.stm

Wark, W.K., 1993, 'The Study of Espionage: Past, Present, Future?', *Intelligence and National Security*, 8, 3, pp.1-13.

Wark, W.K., 2003, 'Learning to Live With Intelligence', *Intelligence and National Security*, 18, 4, pp.1-14.

Warner, M., 2002, 'Wanted: A Definition of Intelligence', *Studies in Intelligence: Journal of the American Intelligence Professional*, 46, 3, pp.15-22.

Warner, M., 2006, 'The Divine Skein: Sun Tzu on Intelligence', *Intelligence and National Security*, 21, 4, pp.483-492.

Warner, M., McDonald, K.J., 2005, *US Intelligence Community Reform Studies Since 1947*, CIA: Centre for the Studies of Intelligence, Washington, available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/US%20Intelligence%20Community%20Reform%20Studies%20Since%201947.pdf

Warren, M.E., (Ed), 1999, *Democracy and Trust*, Cambridge: Cambridge University Press, ISBN:0-521-64687-1.

Watkins, M.D., Bazerman, M.H., 2003, 'Predictable Surprises: The Disasters you Should Have Seen Coming', *Harvard Business Review*, March 2003, pp.72-80.

Waxman, H.A., 2005, *National Security, Emerging Threats and International Relations*, US House of Representatives Committee on Government Reform, Washington.

Weick, K.E., 2003, 'Sense and Reliability', *Harvard Business Review*, April 2003, pp.84-90.

Weller, G.R., 2001, 'The Internal Modernization of Western Intelligence Agencies', *International Journal of Intelligence and CounterIntelligence*, 14, 3, pp.299-322.

Wettering, F.L., 2000, 'Counterintelligence: The Broken Triad', *International Journal of Intelligence and CounterIntelligence*, 13, 3, pp.265-300.

Wettering, F.L., 2001, 'The Internet and the Spy Business', *International Journal of Intelligence and CounterIntelligence*, 14, 3, pp.342-365.

Wheaton, K.J., 2001, *The Warning Solution: Intelligent Analysis in the Age of Information Overload*, Fairfax: AFCEA International Press (AIP), ISBN: 0-916159-30-2.

Wheaton, K.J., 2004, 'The Warning Solution: An Alternative Approach to Early Warning', *Society of Competitive Intelligence Professionals*, 7, 6, pp.6-9.

Wilson, E.O., 2003, *The Future of Life*, (3rd Edition), London: Abacus, ISBN: 0-349-11579-6.

Wilson, P., 2005, 'The Contribution of Intelligence Services to Security Sector Reform', *Conflict, Security and Development*, 5, pp.87-106.

Wilson, P., 2005, 'Intelligence in Practice', unpublished paper supplied to author.

Wlson, M., 2001, *Toward an Ontology of Integrated Intelligence and Conflict*, Decision Support Systems Incorporated, available at: http://www.metatempo.com/DSSIOntology.PDF

Wolf, M., 2004, *Why Globalization Works*, London: Yale University Press, ISBN: 0-300-10252-6.

Wright, G., Bolger, F., Rowe, G., 2002, 'An Empirical Test of the Relative Validity of Expert and Lay Judgements of Risk', *Risk Analysis: An International Journal*, 22, 6, pp.1107-1122.

Wright, S., Badr, A., Weiss, A., Pickton, D., 2004, 'Competitive Intelligence Through UK Eyes', *Journal of Competitive Intelligence and Management*, 2, 2, pp.68-87.

Wriston, W.B., 1986, *Risk and Other Four-Letter Words*, New York: Harper & Row, ISBN: 0-0601-5544-2.

Wyllie, B., 2000, *A Guide to Security Surveys*, Leicester: Perpetuity Press, ISBN: 1-899287-55-8.

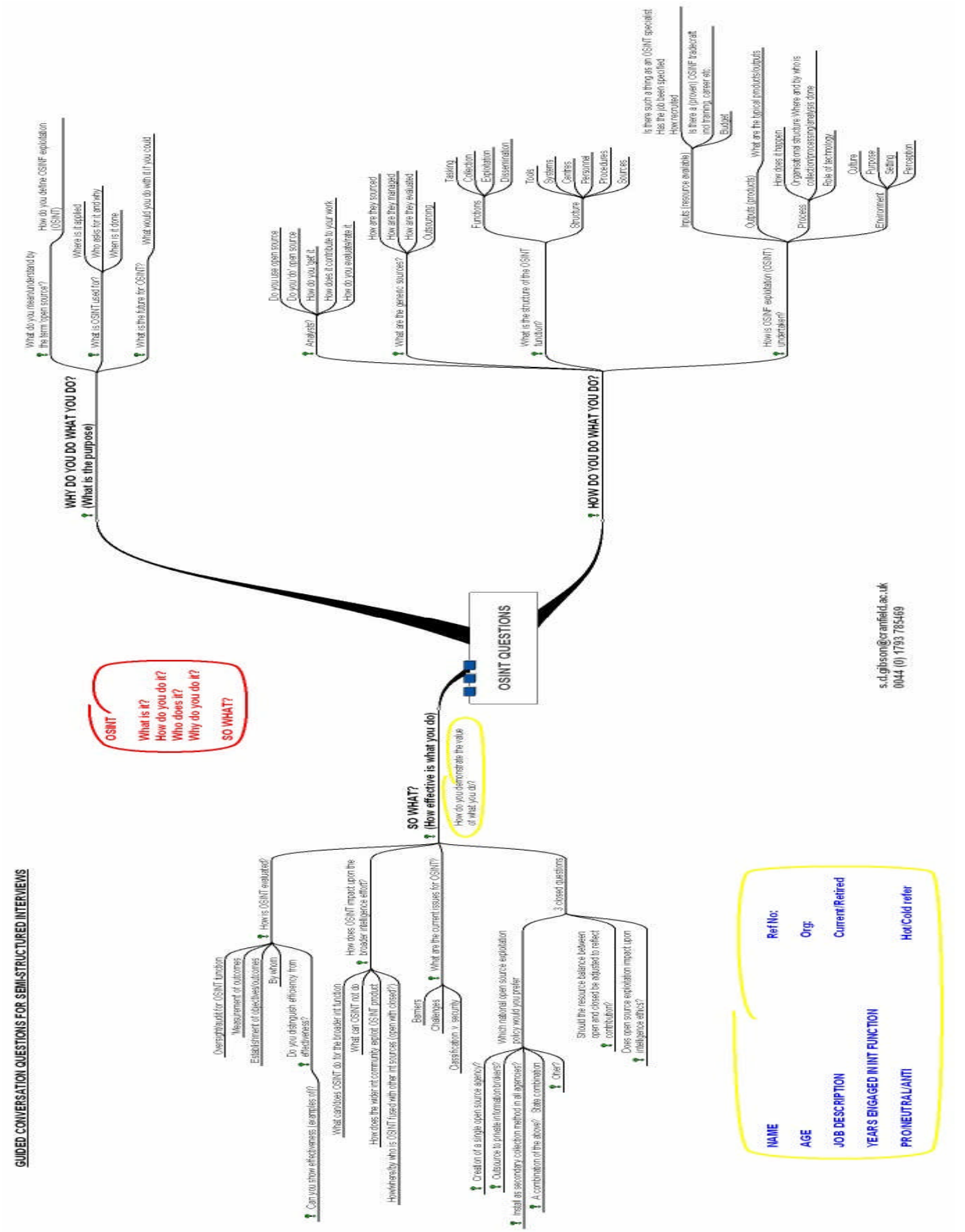
Yin, R.K., 2003, *Case Study Research: Design and Methods*, (Third Edition), London: Sage Publications, ISBN: 0-7619-2552-X.

Zegart, A.B., 1999, *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford: Stanford University Press, ISBN: 0-8047-4131-X.

Zegart, A.B., 2007, '"CNN with Secrets": 9/11, the CIA, and the Organizational Roots of Failure', *International Journal of Intelligence and CounterIntelligence*, 20, 1, pp.18-49.

_____, 2004, 'Intelligence Reform: Centralised Intelligence?', *The Economist*, 11 December 2004, p.50.

APPENDIX A:
INTERVIEW QUESTION MAP
(Guidance for semi-structured interviews)



APPENDIX B.1:
EVALUATION RETURN STATISTICS ON ASD IIRs 1996-2007 (INCLUSIVE)

Grades against years (as totals and percentages)

	IIRs	Total No of evaluations		Major Significance (A)	%	High Value (B)	%	Of Value/Low Value (C/D)	%	No Value (E)	%
1997	640	133	21%	0	0%	64	48%	69	52%	0	0%
1998	619	125	20%	1	1%	74	59%	50	40%	0	0%
1999	426	103	24%	3	3%	58	56%	40	39%	2	2%
2000	381	133	35%	4	3%	72	54%	56	42%	1	1%
2001	635	182	29%	1	1%	122	67%	59	32%	0	0%
2002	511	66	13%	14	21%	23	35%	29	44%	0	0%
2003	436	188	43%	24	13%	65	35%	95	51%	4	2%
2004	493	219	44%	3	1%	85	39%	130	59%	1	0%
2005	425	167	39%	2	1%	63	38%	101	60%	1	1%
2006	391	245	63%	4	2%	133	54%	108	44%	0	0%
Total	4957	1561	31%	56		759		737		9	
Average	991	312	36%	11	5%	152	49%	147	46%	2	1%

APPENDIX B.2:
EVALUATION RETURN STATISTICS ON ASD IIRs 1996-2007 (INCLUSIVE)

Returns from us agencies supplied by year

	1997	1998	1999	2000	2001	2002	2003	2004	2005	2006		
DIA	47	27	25	49	90	4	27	43	20	53	385	24.66%
NGIC	6	8	10	43	40	15	24	18	18	70	252	16.14%
NAIC	0	2	10	12	11	11	105	61	2		214	13.71%
NASIC								49	77	59	185	11.85%
CINCTRANS	45	69	0	0	0	0					114	7.30%
TRANSCOM	4	0	39	6	5	13	3	7	3		80	5.12%
ONI	0	6	1	2	8	3	2	6	18	19	65	4.16%
AFMIC	13	3	6	5	2	2	5	7	1	12	56	3.59%
STRATCOM	0	0	1	2	0	0	3	16	12	6	40	2.56%
NSACSS	0	0	4	3	7	1		4	10	4	33	2.11%
JICPAC	3	3	4	1	2	15		2		1	31	1.99%
JIATF WEST	1	0	0	0	7	0	11	2	2	3	26	1.67%
USARPAC	8	0	1	7	8	0					24	1.54%
CIA	2	1	2	0	1	0	2	1	2		11	0.70%
MSIC	0	0	0	0	0	1	1	1		7	10	0.64%
JWAC								2	1	2	5	0.32%
USDAO HK	4	0	0	0	0	0					4	0.26%
JWAC	0	1	0	0	0	0	3				4	0.26%
US PACOM										3	3	0.19%
KOMUSKOREA	0	0	0	2	0	0					2	0.13%
CIFA										2	2	0.13%
ACIC										2	2	0.13%
AIT	0	1	0	0	0	0					1	0.06%
KUNIA	0	1	0	0	0	0					1	0.06%
AFCENCOM	0	1	0	0	0	0					1	0.06%
SPACECOM	0	1	0	0	0	0					1	0.06%
USSOC	0	1	0	0	0	0					1	0.06%
MDCI	0	0	0	1	0	0					1	0.06%
CDRTACOM	0	0	0	0	1	0					1	0.06%
FMSO	0	0	0	0	0	1					1	0.06%
DOE							1				1	0.06%
US EMBASSY							1				1	0.06%
SOCOM									1		1	0.06%
CENTCOM										1	1	0.06%
MIFCPAC										1	1	0.06%
	133	125	103	133	182	66	188	219	167	245	1561	

BACK COVER