THE UNIVERSITY OF ADELAIDE

School of History and Politics

RETHINKING THREAT:

INTELLIGENCE ANALYSIS, INTENTIONS, CAPABILITIES, AND THE CHALLENGE OF NON-STATE ACTORS

Charles Vandepeer

October 2011

Thesis Declaration

This work contains no material which has been accepted for the award of any other degree or diploma in any university or other tertiary institution to Charles Vandepeer and, to the best of my knowledge and belief, contains no material previously published or written by another person, except where due reference has been made in the text.

I give consent to this copy of my thesis when deposited in the University Library, being made available for loan and photocopying, subject to the provisions of the Copyright Act 1968.

I also give permission for the digital version of my thesis to be made available on the web, via the University's digital research repository, the Library catalogue and also through web search engines, unless permission has been granted by the University to restrict access for a period of time.

Disclaimer

This thesis reflects the author's personal judgments and does not necessarily represent the views of any department or agency of the Australian Government. The author's views should not be attributed to any staff, department or agency of the Australian Government.

Table of Contents

List of Tables **6**
Abstract **7**
Acknowledgements **8**
Introduction **10**
Chapter 1 ..... **16**
Singer's Concept of Threat and the Challenge of Non-State Actors **16**
1.1 Singer's Concept of Threat 16
1.2 Assessing State-Based Threats 21
1.3 The Challenge of Non-State Actors and the Expectations of Intelligence 29
1.4 The Persistence of Singer's Model: Assessing Non-State Threats 37
1.5 Intelligence Analysis: An Under-Theorised Field of Research 44
Chapter 2: The Ontology, Epistemology and Methodology of Assessing Threat: State versus Non-State **53**
2.1 Ontology of Threat 53
2.2 Epistemology of Threat Assessment 68
2.3 Methodology of Threat Assessment 78
Chapter 3: A Critique of Singer's Model as Applied to Non-State Actors: The Intangibility of Capability and Intent **99**
3.1 Measures, Proxy-measures and Indicators of Capability and Intent 99
3.2 Measuring the Capability to conduct a mass-casualty attack 99
3.3 Estimating the Intent to conduct a mass-casualty attack 121
3.4 The Post-hoc Use of Capability and Intent 130
Chapter 4: A Critique of Singer's Model as Applied to Non-State Actors: Towards a More Comprehensive Concept of Threat **133**
4.1 Critiques of Singer's Model 133
4.2 Alternative Approaches for Assessing Threat 136
4.2.1 Vulnerability Approach to Threat 137
4.2.2 Environmental Approach to Threat 142
4.2.3 Situational Approach to Threat 157
4.3 Towards a More Comprehensive Model of Threat 165
4.4 Puzzles, Mysteries and Complexities 166
Chapter 5: Intelligence analysis and the 2001 attacks on New York and Washington **174**
5.1 The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001 174
5.2 Ontology of Threat 176
5.3 Epistemology of Threat 185
5.4 Methodology of Threat Assessment 190
5.5 A More Comprehensive Model of Threat 207
Chapter 6: Intelligence analysis and the 2002 Bali bombings **209**
6.1 Australian Senate Inquiry into Security threats to Australians in Southeast Asia 209
6.2 Ontology of Threat 210
6.3 Epistemology of Threat 222
6.4 Methodology of Threat Assessment 228
6.5 A More Comprehensive Model of Threat 237

Chapter 7: Intelligence analysis and the 2005 London bombings 239
7.1 Investigations into the 7 July 2005 bombings 239
7.2 Ontology of Threat..... 241
7.3 Epistemology of Threat 250
7.4 Methodology of Threat Assessment 255
7.5 A More Comprehensive Model of Threat..... 262
Chapter 8: A critique of Singer's model in practice 264
8.1 Comparison and contrast of incidents..... 265
8.2 Limitations of Singer's model in practice..... 275
8.3 A More Comprehensive Model of Threat..... 282
Conclusion 283
Bibliography..... 286

List of Tables

Table 1: Ontology of Threat: Threat Actors and Referents……58
Table 2: Nature of three incidents by Threat Actor, Location, Nature and Referent……237

Abstract

Recommendations for critical examinations of existing analytical approaches have become a consistent feature of the intelligence literature. Many of these are based on the recognition of an increasingly complex security environment in which non-state actors threaten states' citizens. The publication of previously classified information, particularly following successful mass-casualty attacks, provides an opportunity for critically reviewing approaches to intelligence analysis. Within this context, this thesis critiques a foundational approach to intelligence analysis, namely a conceptual model of threat based on the dual-parameters of intentions and capabilities. This conventional approach was publicly described by J. David Singer in his 1958 seminal paper *Threat Perception and the Armament-Tension Dilemma*. Singer describes government and intelligence agencies' perceptions of threat as being based on the parameters of *capability* and *intent*, displaying the relationship as a quasi-mathematical model: *Threat-Perception = Estimated Capability x Estimated Intent*. This thesis demonstrates this approach has been consistently used by governments, intelligence agencies and within the broader intelligence literature over the past five decades, and was already well-established within intelligence agencies long before Singer described the approach. The study also shows that, despite significant changes in the nature and characteristics of threats, this conventional approach to assessing threat has undergone little modification and limited critique. The core argument of this thesis is that the conventional model used by intelligence agencies is too simplistic to capture the nature and complexity of non-state threats. By articulating an ontology, epistemology and methodology of threat and threat assessment, this thesis moves beyond an uncritical acceptance of the conventional model of threat. The study demonstrates how the model of threat, used and reinforced by intelligence agencies within a Cold War context to assess threats from clearly defined states, has become the primary approach to assessing threats from often ill-defined and amorphous non-state actors. The study specifically focuses on intelligence analysis within the United States, the United Kingdom and Australia which have all demonstrated an acceptance and use of the conventional model of threat against both state-based, and most recently, non-state threats. Each of these states suffered mass-casualty attacks against their citizens from non-state actors within a four year period (2001-2005): the September 2001 attacks in New York and Washington; October 2002 bombings in Bali, Indonesia; and the July 2005 attacks in London. In applying Singer's model to these incidents, the thesis vivifies the analytical challenge of non-state threats in distinct and faceted ways and identifies limitations of the conventional approach when assessing mass-casualty threats from non-state actors.

Acknowledgements

Undertaking a Doctorate is a long, challenging and ultimately rewarding intellectual journey. Along the way I have been assisted by numerous people who have provided me with their time, support, insights and counsel. Additionally, I have been extremely fortunate to have been simultaneously involved in three distinct research fields during my candidature: defence science; military intelligence; and academia. The opportunity to work with people in each of these fields has proven extremely valuable in conceptualising and articulating the kinds of multi-disciplinary problems presented in this thesis.

Professor Felix Patrikeeff, thank you for your ongoing supervision throughout this thesis. As a part-time student, the last six years have provided me with an invaluable experience. Through your supervision I was given an opportunity to develop and gain deep insights into a broad range of intellectual and academic areas. Thank you also for giving me a foundation from which to discover and develop new ideas and skills whilst also ensuring that I remained on track to achieving the aims and goals for the research. It has been excellent working with you and I look forward to continuing the research relationship well into the future.

Dr David Matthews, as co-supervisor your support and insights have been outstanding and greatly appreciated. You have been a constant source of encouragement as well as someone who provided rigorous debate, critique, guidance and invaluable suggestions. Thanks to you and your family for opening your house to me whilst in the UK as well as the many hours that you have invested into reviewing and discussing the arguments contained herein.

Dr Wayne Hobbs, for your ongoing support, interest and assistance in securing time to pursue this research. Dr Terry Moon for your continued motivation, advice and suggested future directions which proved invaluable. Dr Coen Van Antwerpen for your support and recognising potential. Dr Wayne Philp, your original advice to invest in a PhD has proven to be such a worthwhile endeavour. David Olney, it has been a pleasure lecturing with you and the many hours of discussion and insight have been invaluable. Michael O'Byrne who forced me to write up what would became the initial scoping paper for the research. Commander Dina Kinsman for your advice on honing my writing skills. Dr Lucy Resnyansky for your ongoing encouragement, open door and advice. Cliff White, Dr Richard Price and Dr Mike Davies for your support for the thesis at the very outset and your efforts at garnering support for this research. The ability to work in a multi-disciplinary team at DSTO has been an excellent experience, and my thanks to the entire team for exposing me to methodologies from across a range scientific fields. To Bruce for the reviews, logic checks and feedback throughout the project which were all greatly appreciated. Also to Simon Pope and Jason Sargent, for your consistent encouragement and motivation towards completing the thesis. The efforts of all of the Library Staff at DSTO Edinburgh have also been invaluable in tracking down difficult-to-acquire material in a very timely manner.

Along the way I have been fortunate to debate, discuss and present my research to a number of leaders and thinkers in a number of fields. I am indebted to each of these busy people for generously giving me their time, thoughts and the opportunity to discuss and debate many of the arguments that appear in this thesis. These people have included: Dr

Brian Jackson, Dr James Bruce, Gregory Treverton and Dr Bruce Bennett, Richards Heuer, Barton Whaley, Lieutenant Colonel David Kilcullen PhD, Lieutenant Colonel Ian Wing PhD, Alfred Rolington, Josh Kerbel, Professor Andrew O'Neil, Professor Mark Phythian, Brigadier Andrew Smith PhD, Brigadier David Gillian, Anthony Bill, and David Snowden.

I would also like to thank a number of people for the openings and opportunities that I have been provided during the completion of this thesis. Major General Maurice McNarn, Brigadier Gary Hogan and Peter Bunyan who provided me with the invitation to present my work to Agencies, also for the external support for the research and securing me an invitation to Singapore's inaugural International Risk Assessment and Horizon Scanning Symposium. Wing Commander Trotman-Dickenson for his leadership and the many opportunities to achieve numerous career ambitions. To the many RAAF intelligence officers whom I have discussed and debated my research with and to the men and women of 87 Squadron for the work that they do. To Harry Shukman and for his interest and encouragement. Roy Giles for his zeal and drive in establishing Project GOA and providing a place to stay during its launch in Oxford. The members of Project GOA and the Oxford Intelligence Group for their support. Michael Herman at Nuffield College for his time and insights. To Dr Hank Prunken and Patrick Walsh, Australian authors in the intelligence field, who have provided a consistent source of encouragement throughout. I would also like to recognise the early teachings of Craig Phasey and Graeme Clarke.

To M.R. and my family who have been a constant source of encouragement and inspiration throughout.

Introduction

> Intelligence merely provides techniques for improving the basis of knowledge. As with other techniques, it can be a dangerous tool if its limitations are not recognised by those who seek to use it.
>
> Lord Butler[1]

> A threat consists of capabilities multiplied by intentions; if either one is zero, the threat is zero.
>
> Richard Betts[2]

Recommendations for critical examinations of existing analytical approaches have become a consistent feature of the intelligence literature.[3] Many of these are based on the recognition that the immediate security concerns for countries and their citizenry are not confined to threats from other states. These arguments gain weight in light of the shifting priorities of governments themselves, with non-state actors becoming an increased concern for intelligence agencies. At the same time, increased media coverage and public awareness of intelligence, particularly following mass-casualty attacks, has prompted

[1] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.14-15.
[2] Richard Betts, Intelligence Warning: Old Problems, New Agendas, *Parameters*, Spring 1998, pp.26-35.
[3] For example, see: Richards Heuer, Limits of Intelligence Analysis, *Orbis*, Vol.49, No.1, Winter 2005, pp. 75-94, p.94; Frederick Hitz and Brian Weiss, Helping the CIA and FBI Connect the Dots in the War on Terror, *International Journal of Intelligence and Counter Intelligence*, Vol.17, 2004, pp.1-41, p.29; Bruce Berkowitz, Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, pp.289-300, p.289; Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53; Alfred Rolington, Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.738-759, p.745; and Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.36.

governments to release intelligence analysis and assessments within years (even months) of actual events. The publication of previously classified information has enabled a more rigorous examination of intelligence analysis closer to the actual events than would have previously been achievable.[4] These factors provide both an opportunity and an impetus for critically reviewing approaches to intelligence analysis. Given that the primary focus of intelligence is the identification and assessment of threat, it appears timely to re-think a foundational principal of intelligence analysis: a concept of threat based on the parameters of intentions and capabilities.[5]

Within the field of intelligence studies, there is a remarkably consistent and enduring concept of threat. This concept was described and defined in J. David Singer's 1958 seminal paper *Threat Perception and the Armament-Tension Dilemma,* which provides a definition of threat perception as consisting of the two parameters of *capability* and *intent*.[6] Singer displays the relationship as a quasi-mathematical model: *Threat-Perception = Estimated Capability x Estimated Intent*. Singer's threat equation publicised and codified a concept of threat *already* established and being used within intelligence agencies in the United Kingdom and the United States.[7] Declassified intelligence analysis, government

[4] In the United Kingdom and Australia a thirty-year rule is applied to classified information as a standard; even then, some classified information might not be released based on a perception of the sensitivity of the subject matter. Consequently, the lack of timeliness with release of previously classified information potentially limits the value of the type of critical examination that the academic community could bring to the field.

[5] In terms of *types* of threat, this thesis (and the majority of the references cited herein) discusses threat in terms of direct threat of *conflict, war or violence* as opposed to *economic* or *espionage* threats, though the intentions-capability model could also be applied within these contexts of threat. A discussion of referents of threat and threat actors is included in Chapter 2.

[6] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.

[7] For declassified US examples, see: National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950 (acknolweding that this was a policy document rather than a formal intelligence assessment); Central Intelligence Agency, *Possibility of Direct Soviet Military Action During 1948*, ORE 22-48, 2 April 1948; Central Intelligence Agency, *Estimate of the Effects of the Soviet Possession of the Atomic Bomb upon the Security of the United States and upon the Probabilities of Direct Soviet Military Action*, ORE 91-49, 6 April 1950; and Central Intelligence Agency, *Soviet Capabilities and*

publications and the intelligence literature illustrate that, for at least the last sixty years, assessments of threats have been largely based upon the model described by Singer.[8] This thesis does not argue that analysts or academics have applied this intentions-capability approach in a quasi-mathematical approach as presented by Singer, though as will be shown some have referred to it in such similar terms. Instead, as is demonstrated in this thesis, these two parameters have formed the basis and conceptual framework for assessing threats within intelligence analysis for decades. Despite significant changes in the nature and characteristics of threats, this conventional approach to assessing threat has undergone little modification and limited critique over the last five decades. Thus, this conceptual model of threat continues to be adopted within government intelligence agencies and the broader academic literature, re-enforcing the traditional concept in the minds of new analysts and researchers entering the field.[9]

The core argument of this thesis is that this conventional model is too simplistic to capture the nature and complexity of non-state threats.[10] The model was originally used to assess threats from clearly defined states and was not intended to be applied to threats from often

---

Intentions, National Intelligence Estimate NIE-3, 15 November 1950; and *National Security Act of July 26, 1947*. For declassified British examples refer to: Joint Intelligence Committee, *Soviet Interests, Intentions and Capabilities -General*, JI (47) 7/2 Final, 6 August 1947; Joint Intelligence Committee, *The Soviet Threat*, JIC (51) 6, London PRO, CAB 158/12, 19 Jan 1951. For declassified Australian examples refer to: Defence Committee, *A Strategic Basis of Australian Defence Policy*, Defence Committee Report, 8 January 1953; Joint Intelligence Committee, *Intelligence Aspects of the Strategic Basis for Australian Defence Policy*, JIC (M) 35 August 1956; and Defence Committee, *Strategic Basis of Australian Defence Policy*, December 1958.

[8] This 'intentions-capability' approach to threat assessment is referred to in this thesis as 'Singer's model'.

[9] Glen Segell, Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004, *International Journal of Intelligence and Counterintelligence*, Vol.18, No.2, pp.221-238, pp.224-225. Richards Heuer's *The Psychology of Intelligence Analysis* and Richard K Betts's *Analysis, War and Decision: Why Intelligence Failures are Inevitable*, arguably the two most cited texts within the field of intelligence analysis, both adopt the concept of threat in terms of the parameters *intent* and *capability*. For use in government intelligence agencies, refer to: United Kingdom Government, *Threat Levels: The System to Assess the Threat from International Terrorism*, The Stationery Office, London, July 2006, p.2; Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/index.htm; and National Intelligence Council, *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007.

[10] I define a model as a conceptual framework or mental construct.

ill-defined and amorphous non-state actors. This thesis demonstrates that the intelligence literature lacks deliberate critiques over the assumptions, limitations or consequences of applying a state-based methodology to the assessment of non-state threats.

The study specifically focuses on intelligence analysis within Australia, the United Kingdom and the United States.[11] Governments and intelligence agencies in these three countries display long-standing acceptance and use of the conventional model of threat in assessing both state-based and non-state threats. Additionally, these states also suffered mass-casualty attacks against their citizens from non-state actors within a four year period (2001-2005). In September 2001, nineteen men with links to Al Qa'ida flew two hijacked planes into the two World Trade Centre buildings in New York and a third into the Pentagon in Washington, D.C.[12] Nearly 3,000 people were killed in the largest attack on the United States by a non-state actor. The scale and coordination of the attacks, emphasised by live media coverage of the second plane hitting the World Trade centre and the two buildings' subsequent collapse, had a profound impact on the United States as well as governments and citizens around the globe. The attacks single-handedly reframed perceptions of non-state threats. Eleven months later, in October 2002, members of Jemaah Islamiyah (JI) detonated two bombs on the Indonesian island of Bali, at the time the most popular overseas tourist destination for Australians. Of the 202 people killed in the attacks, Australia suffered the highest number of casualties, with 88 citizens killed. The Bali attacks killed more Australians than any other single attack by a non-state actor in the country's history. Almost three years later, in July 2005, four British citizens conducted

[11] As intelligence analysis occurs within government agencies a great deal of the thesis draws, unapologetically, from governments and intelligence agencies' own descriptions of threat through publications, testimonies and declassified analysis.

[12] A fourth hijacked plane crashed in a field northwest of Washington D.C. following an attempt by passengers onboard to regain control of the aircraft.

suicide attacks on the London public transport system, killing 56 people. These individuals were able to use home-made bombs to carry out the largest attack in London since World War Two. The individuals' links with Al Qa'ida are assessed as likely, but (at the time of writing) the nature of these links is still unable to be confirmed.[13] Examining each of these three incidents vivifies the problem of non-state threats in distinct and faceted ways.

In response to these attacks, formal inquiries or investigations were undertaken resulting in the release of previously classified analysis and providing insight into what intelligence agencies knew about these threats and how they were assessing non-state actors prior to the attacks. Each of these incidents highlighted similar facets of the analytical difficulty of assessing non-state threats, whilst also raising unique aspects of the problem. In applying Singer's model to these incidents, the study illuminates limitations of the approach when applied to assessing the threat of mass-casualty attacks by non-state actors.

The model of threat described by Singer is a foundational concept within intelligence literature. Consequently, in lieu of a conventional literature review, Chapter 1 demonstrates the near-universal acceptance of the model by practitioners and academics alike and illustrates how this study fills a void in the current literature. The ontology, epistemology and methodology of state-based and non-state threat and threat assessment are discussed in Chapter 2. The chapter also explores the context of the application of the model and surfaces assumptions underpinning the approach. Chapter 3 re-engages with the parameters of the conventional approach, specifically examining the measures, proxy-measures and indicators identified within the literature upon which assessments of non-state actors'

[13] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.101.

capabilities and intentions are based. The limited literature critiquing the conventional threat model is detailed in Chapter 4 before considering alternatives to the popular actor-based approach. Finally, chapters 5-7 build upon the previous chapters by applying Singer's model to: the 2001 attacks on New York and Washington; the 2002 attacks in Bali, Indonesia; and the 2005 bombings in London. These chapters illuminate a number of similar and unique aspects of the analytical problem and identify limitations to the conventional model when applied to assessments of non-state threat.

Chapter 1

Singer's Concept of Threat and the Challenge of Non-State Actors

> One of the most important, yet daunting, tasks for intelligence analysts is to gauge enemy political intentions and military capabilities. Analysts need to marry political-intention and military-capability assessments to form a threat assessment for policymakers.
>
> Richard Russell[1]

> At the core of intelligence is the challenge of analysis.
>
> Loch Johnson[2]

1.1 Singer's Concept of Threat

When looking at the intelligence literature, it quickly becomes apparent that a consistent concept of threat runs through intelligence. This concept of threat is reflected in J. David Singer's 1958 seminal paper, *Threat-perception and the armament tension dilemma*. Singer provides a definition of threats from states as consisting of both an estimated capability and an estimated intent, displaying the relationship as a quasi-mathematical model: *Threat-Perception = Estimated Capability x Estimated Intent*.[3] As is shown in the following paragraphs, at the time of publication, the concept of threat described by Singer was *already* well-established and adopted within intelligence agencies. Further, Singer's work was not the first to publish a concept of threat based upon the parameters of *intentions* and *capabilities* within the academic literature. Schwien's 1936 publication

[1] Richard Russell, Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities, in Loch Johnson (Ed.), *The Oxford handbook of national security intelligence*, Oxford University Press, Oxford, 2010, p.375.
[2] Loch Johnson, An Introduction to the Intelligence Studies Literature, in *Strategic Intelligence 1: Understanding the Hidden Side of Government*, ed. Loch Johnson, Praeger Security International, Westport, 2007, p.5.
[3] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.

Combat Intelligence: Its Acquisition and Transmission, considered the challenge of capabilities versus intentions in reviewing the German Second Army on the battlefield at the start of World War One.[4] The development of formal intelligence agencies, as well as the move towards examining states as a whole, appears to have influenced this capabilities and intentions approach to assessing actual or potential state-based threats. Up until 1945, Michael Herman argues that "…assessing states in the round evolved out of the need to view enemies and potential enemies in terms of national capabilities and intentions as well as traditional military yardsticks".[5] What makes Singer's paper notable is that it was published in the available literature as well as the manner in which he presented this dual-parameter concept. Singer was the first to display this concept as a quasi-mathematical (and memorable) equation for assessing threat, introducing this model of threat assessment into public debate. This intentions-capability approach to threat described by Singer has undergone limited modification over the last fifty years, remaining recognisable in its numerous appearances in both declassified intelligence assessment as well as the academic literature on intelligence and security. This is not to suggest that there are not variations on this concept of threat.[6] Most notably, the additional parameters of *opportunity* and

[4] Edwin Schwien, *Combat Intelligence: Its Acquisition and Transmission*, Washington, D.C., The Infantry Journal Inc., 1936, pp.8-26. Within British intelligence, prior to outbreak of the Second World War, there appeared to be a move towards this conceptual approach of examining threats from the perspective of both capabilities and intentions. Michael Goodman argues that between 1909 (with the establishment of MI5) and "…really up until the outbreak of the Second World War, British intelligence was a purely military discipline. Not only were both departments staffed by military figures, but also their outlook was solely military: they were interested in enemy capabilities and nothing whatsoever to do with political or enemy intentions. This process gradually began to change from the mid-1920s onwards". Michael Goodman, The British Way in Intelligence, in Matthew Grant (Ed.), *The British way in cold warfare: intelligence, diplomacy and the bomb, 1945-1975*, Continuum, London, 2009, p.130.

[5] Michael Herman, *Intelligence power in peace and war*, University of Cambridge, Cambridge, 1996, p.259. In discussing the integration of intelligence and emergence of "'national assessments', or seeing the enemy as a whole", Herman argues that: "[a]fter 1945 the Cold War gave special relevance to this lesson in both Britain and the United States. The communist threat seemed to span political, military, economic and subversive attacks, and needed equally comprehensive intelligence assessment. The intentions and capabilities of the intensely secretive Soviet and Chinese regimes had to be studied by putting together evidence from all sources and sectors". *Ibid.*, Pp25-26.

[6] This thesis avoids a debate over semantics, noting that similar terms can be, have been, and are often used in place of *capability* and *intent*, such as *means* and *will*, as these words are often used interchangeably

vulnerability, discussed in detail in Chapter 2, regularly appear within the literature in an apparent attempt to capture the breadth of the subject of threat. However, the parameters of *opportunity* and *vulnerability* do not replace the parameters *intent* and *capability* but exist as additions to them. Thus, irrespective of additional parameters, the parameters of intent and capability form a consistent and recognisable concept of threat within intelligence agencies and the literature on intelligence. Unfortunately, despite its frequent usage in intelligence analysis since (at least) before World War Two, the origins, context, application and assumptions behind this dominant dual-parameter approach to assessing threat has itself undergone limited critique or consideration within the field of intelligence. This use of concepts and terms without awareness or consideration of their original usage or conceptual underpinnings is not without precedence within the intelligence field. For example, despite the popularity of the concepts of 'mysteries' versus 'puzzles' or 'secrets' in describing intelligence problems, most commentators and officials employing these conceptualisations appear unaware of their intellectual origins or conceptual underpinnings.[7] Indeed, as Odom observes "…analysts must work within organisations locked in preconceptions and strong normative biases. Inevitably they will absorb many of those biases".[8] It is argued that the concept of threat *described* by Singer is one such conceptual approach.

Before commencing with a discussion of the application of the model described by Singer, it is important to demonstrate that *threat* constitutes the principal focus of intelligence

---

(regularly in the same document) to mean the same thing.

[7] A discussion of 'mysteries' and 'puzzles' or 'secrets' as an epistemological approach to analysis is discussed in detail in Chapter 4. Of all commentators using the term, it appears that only Gregory Treverton links these concepts with Horst Rittel and Melvin Webber, Dilemmas in a General Theory of Planning, *Policy Sciences*, Vol.4, 1973, pp.155-169.

[8] William Odom, Intelligence Analysis, *Intelligence and National Security*, Vol.23, No.3, pp.316-332, pp.326-327.

agencies. The argument is that identification and accurate assessment of threat is the *raison d'etre* of intelligence. The centrality of threat within intelligence is argued by Ken Robertson in his effort at defining intelligence, arguing that:

> A satisfactory definition of intelligence ought to make reference to the following: threats, states, secrecy, collection, analysis, and purpose. The most important of these is threat, since without threats there would be no need for intelligence services.[9]

This core focus on threat, and threat assessment, is demonstrable by both the contexts within which formal intelligence agencies have been established in the 20th and 21st centuries as well as government legislation on intelligence. The establishment of intelligence agencies within the UK and US highlight the centrality of perceptions of threat, and a desire to ensure that states are not surprised. The establishment of the Britain's Secret Service Bureau (forerunner to MI5 and MI6) in 1909 was as a response to fears about a Germany invasion and that state's espionage activities.[10] Britain's Joint Intelligence Committee (JIC) was established in 1936 to provide central direction for intelligence against the backdrop of "a darkening international environment".[11] Consequently, Percy Cradock notes that the agency "has a predilection for the threats rather than the opportunities, for the dark side of the moon".[12] The United States established the Central Intelligence Agency in 1947 out of the profound shock of the surprise attack by Japan at Pearl Harbour, the experience of World War Two against the

[9] Ken Robertson, 'Intelligence, Terrorism and Civil Liberties', *Conflict Quarterly*, Vol.7, No.2, Spring, 187, p.46, quoted in Michael Herman, *Intelligence power in peace and war*, Cambridge University Press, Cambridge, 1996, p.118.
[10] Michael Goodman, Learning to Walk: The Origins of the UK's Joint Intelligence Committee, *International Journal of Intelligence and CounterIntelligence*, Vol.21, 2008, pp.40–56, p.40.
[11] Percy Cradock, *Know Your Enemy: How the Joint Intelligence Committee Saw the World*, John Murray, London, 2002, p.7.
[12] *Ibid*., p.4.

Axis powers, and the perceived threat from the Soviet Union.[13] The US Department of Homeland Security emerged from the 11 September 2001 attacks, with an increased perceived threat of such types of attacks critical in the establishment of UK's Joint Terrorist Analysis Centre and Australia's National Terrorist Analysis Centre. State legislation on intelligence also highlights how parameters used to define *threat* have also been used by governments to define the purpose of *intelligence*. The following quotes illustrate this point. The United States' current legislation on intelligence agencies, the *National Security Act of 1947,* defines "foreign intelligence" as "information relating to the *capabilities, intentions*, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities".[14] A similar definition is provided within current Australian legislation, with the *Australian Security Intelligence Organisation (ASIO) Act 1979* defining foreign intelligence as "intelligence relating to the *capabilities, intentions* or activities of a foreign power".[15] Similarly, the Australian *Intelligence Services Act 2001* (current legislative act) provides guidance to intelligence collection agencies to obtain "…intelligence about the *capabilities, intentions* or activities of people or organisations outside Australia".[16] The United Kingdom's intelligence and

[13] Richard Immerman, A Brief History of the CIA, Athan Theoharis, Richard Immerman, Loch Johnson, Kathryn Olmsted, and John Prados (Eds.), *The Central Intelligence Agency: Security Under Scrutiny*, Greenwood Press, Westport, 2006, p.2.

[14] National Security Act of July 26, 1947, (as Amended) accessed at: http://www.intelligence.gov/0-natsecact_1947.shtml on 11 April 2008, Sec.3. [50 USC. 401a] (2). Under the Act, "intelligence" includes foreign intelligence and counterintelligence. Sec.3. [50 USC. 401a] (1). Italics added by author.

[15] *The Australian Security Intelligence Organisation Act 1979* (current legislation), defines a foreign power as: (a) a foreign government; (b) an entity that is directed or controlled by a foreign government or governments; or (c) a foreign political organisation. *Australian Security Intelligence Organisation Act 1979*, Act No. 113 of 1979 as amended, Preliminary Part I, Section 4, p.2-3. Italics added by author.

[16] Intelligence Services Act 2001, Act No. 152 of 2001. Within this act, the Defence Signals Directorate is charged with obtaining "…intelligence about the capabilities, intentions or activities of people or organisations outside Australia". Intelligence Services Act 2001, Act No. 152 of 2001 as amended, Part 2, Section 8, p.6-7. The roles of the Australian Secret Intelligence Agency (ASIS) are similarly defined: "…to obtain, in accordance with the Government's requirements, intelligence about the capabilities, intentions or activities of people or organisations outside Australia". Intelligence Services Act 2001, Act No. 152 of 2001 Part 2, Section 6, as amended, p.5. The *Australian Security Intelligence Organisation Act 1979* (current), defines a foreign power as: (a) a foreign government; (b) an entity that is directed or controlled by a foreign government or governments; or (c) a foreign political organisation. *Australian Security Intelligence*

security legislation use the term "intention" and "actions", but not "capability". *Intelligence Services Act 1994*, the Secret Intelligence Service (SIS) is "…to obtain and provide information relating to the actions or *intentions* of persons outside the British Islands…" and "…to perform other tasks relating to the actions or *intentions* of such persons".[17] Given their appearance in legislation, it is perhaps unsurprising that intelligence agencies have adopted similar parameters of intentions and capabilities when assessing both threats from states and non-state actors.[18]

1.2 Assessing State-Based Threats

Declassified intelligence assessments from the early Cold War period through to today illustrate that the dual-parameter threat-perception model described by Singer (hereafter referred to as Singer's model) remains the primary approach used by intelligence agencies to assess state-based threats.[19] Thus, for at least the last sixty years, the model described by

---

Organisation Act 1979, Act No. 113 of 1979 as amended, Preliminary Part I, Section 4, p.2-3. Italics added by author.

[17] *Intelligence Services Act 1994*, Chapter 13,1 (1) (a) (b). Under the same Act, GCHQ is to focus on "…the actions or intentions of persons outside the British Islands". *Intelligence Services Act 1994*, Chapter 13, 3 (2) (b). Italics added by author.

[18] The *intentions* and *capability* approach can be equated with the popular model used by police agencies of "means, motive and opportunity". There is, however, a significant difference between the application of these models. Whilst the model described by Singer is primarily used for assessing current and future threats, the model employed by police is largely used to identify potential suspects to an event which has *already* occurred. Skillicorn highlights this reactive nature of much of law enforcement and prosecution, that it is to "…punish bad activity after it happens, rather than prevent it before it happens". David Skillicorn, *Knowledge Discovery for Counterterrorism and Law Enforcement*, Taylor and Francis, Boca Raton, 2009, p.301.

[19] As noted, Singer describes an approach to threat assessment already in use within intelligence agencies in assessing state-based threats. Additionally, analysts have for decades been exposed to (or trained in) this approach to conceptualising and assessing threats, largely without critique, by intelligence analysts across the United States, United Kingdom and Australia. Consequently, the focus of this thesis is on the pervasiveness and influence 'intent-capability' concept of threat *described* by Singer. The extent of Singer's own influence, or the influence of this 'threat equation' would be impossible to determine, and be of little value. Instead, this thesis demonstrates that that the concept of threat described by Singer is so ingrained and accepted within intelligence analysis usually devoid of critique or consideration of underpinning assumptions. For ease of reference, this thesis refers to this conceptual model of threat as *Singer's model* in that it is the dominant model of threat *described* by Singer. Such an observation of analysts being influenced by the concepts accepted within agencies, without necessarily questioning the dominant approach, is echoed in Odom's discussion of analysts and normative biases, as discussed earlier. Odom observes that "…analysts must work within organisations locked in preconceptions and strong normative biases. Inevitably they will absorb many of those biases". It is argued that the concept of threat described by Singer is one such conceptual approach.

Singer has influenced American, British and Australian analysts' assessments of threat. This inability to conceptualise threat through alternative concepts could be seen as a weakness within both intelligence communities as well as the broader literature. Declassified by British, American and Australian intelligence assessments from the Cold War highlight the singular reliance on this conventional model of threat for assessing threats from states.[20] The quotes which follow underscore this observation.

In the United States, the influential 1950 *NSC-68: United States Objectives and Programs for National Security* provided to President Truman employed this concept as a frame through which to assess the threat from the Soviet Union.[21] NSC-68 described the threat from the Soviet Union in terms of "Soviet *intentions* and *capabilities*", directly contrasting these with "US *intentions* and *capabilities*", including a "Military Evaluation of US and USSR Atomic *Capabilities*".[22] Matthew Perl's comparison of the US NSC-68 with and UK intelligence assessments at the time finds that there was agreement in American and British assessments of the Soviet Union's capabilities, but differences in their assessments

---

William Odom, Intelligence Analysis, *Intelligence and National Security*, Vol.23, No.3, pp.316-332, pp.326-327.

[20] For declassified US examples, see: National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950; Central Intelligence Agency, *Possibility of Direct Soviet Military Action During 1948*, ORE 22-48, 2 April 1948; Central Intelligence Agency, *Estimate of the Effects of the Soviet Possession of the Atomic Bomb upon the Security of the United States and upon the Probabilities of Direct Soviet Military Action*, ORE 91-49, 6 April 1950; and Central Intelligence Agency, *Soviet Capabilities and Intentions*, National Intelligence Estimate NIE-3, 15 November 1950. NIE-3 defines the analytical problem addressed by the Estimate within the construct of the conventional model of threat: "To estimate Soviet capabilities and intentions with particular reference to the date at which the USSR might be prepared to engage in a general war". For declassified British examples refer to: Joint Intelligence Committee, *Soviet Interests, Intentions and Capabilities -General*, JIC (47) 7/2 Final, 6 August 1947; Joint Intelligence Committee, *The Soviet Threat*, JIC (51) 6, London PRO, CAB 158/12, 19 Jan 1951. For declassified Australian examples refer to: Defence Committee, *A Strategic Basis of Australian Defence Policy*, Defence Committee Report, 8 January 1953; Joint Intelligence Committee, *Intelligence Aspects of the Strategic Basis for Australian Defence Policy*, JIC (M) 35 August 1956; and Defence Committee, *Strategic Basis of Australian Defence Policy*, December 1958. Italics added by author.

[21] National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950, accessed 31 October 2007 at: www.fas.org/irp/offdocs/nsc-hst/nsc-68-1.htm

[22] For the contrasting assessments of USSR and US intentions and capabilities refer to Sections 5-6 of the National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950, accessed 31 October 2007 at: www.fas.org/irp/offdocs/nsc-hst/nsc-68-1.htm. Italics added by author.

of Soviet intentions.[23] What Perl's analysis reveals, albeit without consciously addressing the issue, is that, by the late 1940s and early 1950s, the US and UK had adopted an identical analytical approach to assessing threats.[24] For example, the Central Intelligence Agency's 1950 report (ORE 91-49) discusses the threat of the Soviet Union's possession of an atomic weapon in terms of assessments of "Soviet Atomic *Capabilities*" and an "Estimate of Soviet *intentions* and objectives".[25] Similarly, the CIA's National Intelligence Estimate (NIE-3), of 15 November 1950, defines the reports analytical problem as "[t]o estimate Soviet *capabilities* and *intentions* with particular reference to the date at which the USSR might be prepared to engage in a general war".[26] In comparison, the United Kingdom's Joint Intelligence Committee (JIC) 1947 assessment *Soviet Interests, Intentions and Capabilities* described the Soviet threat in terms of: "*capabilities*" (economic potential and capacity to wage war); "General Soviet policy" (based upon assessments of Soviet Government's plans to achieve security); and "Soviet interests and *intentions*" towards broad geo-political regions.[27] As noted by Peter Hennessey, "[a] pronounced feature of the JIC's large surveys of Soviet *intentions* and *capabilities* was their area-by-area, often country-by-country, examination of Soviet influence and the likely location of potential hot spots".[28] That was not to suggest that British intelligence was able to confidently or

[23] Perl argues that the basis of US assessments of intentions differed from British assessments because of the factors considered. Perl notes that the US intelligence agencies "…*assumed* Soviet intentions based on an interpretation of Communist ideology". In contrast the British intelligence assessments "…rigorously examined and *analysed* the USSR's intentions based on several factors including, crucially, Soviet actions". Matthew Perl, Comparing US and UK Intelligence Assessment in the Early Cold War: NSC-68, April 1950, *Intelligence and National Security*, Vol.18, No.1, 2003, pp.119-154, p.146. Italics as per original.

[24] Declassified British intelligence assessments indicate agencies were formally assessing state-based threats using such parameters at least as early as 1928. See Committee of Imperial Defence, *The Military Situation in Germany*, CID Paper 926B, 11 December 1928.

[25] Central Intelligence Agency, *Estimate of the Effects of the Soviet Possession of the Atomic Bomb upon the Security of the United States and upon the Probabilities of Direct Soviet Military Action*, ORE 91-49, 6 April 1950. Italics added by author.

[26] Central Intelligence Agency, *Soviet Capabilities and Intentions*, National Intelligence Estimate NIE-3, 15 November 1950. Italics added by author.

[27] Joint Intelligence Committee, *Soviet Interests, Intentions and Capabilities -General*, JIC (47) 7/2 Final, 6 August 1947. Italics added by author.

[28] Peter Hennessey, *The Secret State: Whitehall and the Cold* War, Penguin Books, London, 2003, p.24.

accurately assess the threat from the Soviet Union. As Peter Davies notes, "[a]fter the Second World War when the Soviet Union emerged as the principal threat to the UK, the British government's stock of intelligence on Soviet intentions and capabilities was 'alarmingly inadequate'".[29]

The argument has been made that the focus on intentions and capabilities of the Soviet Union dominated thinking in both the British and United States intelligence communities. Indeed, so ingrained was this intentions and capabilities approach, that it was (and continues to be) regularly used to describe the *purpose* of US and British intelligence agencies. As an example, in discussing the close links between UK and US intelligence agencies, Richard Aldrich frames their objective in terms of the conceptual approach, arguing that "[t]he central objective of these intelligence communities has been to offer precise estimates of the capabilities of opponents and timely warning of their intentions".[30] Interestingly, Aldrich also observes that "American estimates of Soviet capabilities and intentions, unlike British ones, have long been a subject of study".[31] In considering intelligence in the 1950s, Walter Laqueur argues that "…Soviet military *capabilities* and *intentions* remains the most important topic for American intelligence".[32] Such an argument was apparent in the 1954 Doolittle Commission on the covert activities of the CIA, which stated that "[t]he acquisition and proper evaluation of adequate and reliable intelligence on the capabilities and intentions of Soviet Russia is today's most important

---

Italics added by author. b

[29] Pete Davies, The British Way of Economic Intelligence during the Cold War in Matthew Grant (Ed.), *The British way in cold warfare: intelligence, diplomacy and the bomb, 1945-1975*, Continuum, London, 2009, p.177.

[30] Richard Aldrich, British intelligence and the Anglo-American 'Special Relationship' during the Cold War, *Review of International Studies*, Vol.24, 2008, pp.331–351, p.331.

[31] Richard Aldrich, British intelligence and the Anglo-American 'Special Relationship' during the Cold War, *Review of International Studies*, Vol.24, 2008, pp.331–351, p.332.

[32] Walter Laqueur, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, 1993, p.116. Italics added by author.

military and political requirement".[33] Some fifty years later, Lord Butler makes a similar observation in relation to British intelligence, arguing that, for the duration of the Cold War, "…the intelligence community's major task was to assess the *intentions* and *capabilities* of the Soviet Union and its satellite states".[34] Similarly, Matthew Grant observes that "[a] central part of the 'British way' in Cold Warfare was to analyse the enemy's *intentions* and *capabilities* in order to better understand their policies, and to inform Britain's own".[35] Michael Goodman captures the approach employed by Britain's Joint Intelligence Committee in assessing threats from other states, noting that "[i]n considering the preparations by various countries to launch acts of aggression, the JIC had to distinguish between intentions and capabilities: that is, whether a country had the political will to launch an attack, and whether they had the practical means to do so".[36] Based upon the review of thousands of declassified British intelligence reports in the British National Archives, the conclusion of Stephen Robert Twigge, Graham Macklin, Edward Hampshire on British Cold War intelligence is revealing. Twigge *et al.* observe that "[d]uring the Cold War, the threat of surprise attack was a constant and inevitable concern. As a result, the intelligence community's major task was to assess the *intentions* and *capabilities* of the Soviet Union, particularly its nuclear arsenal".[37] Consequently, "[m]onitoring Soviet *capabilities* and *intentions* was a prime objective of British

[33] Report of the Special Study Group [Doolittle Committee] on the Covert Activities of the Central Intelligence Agency, 30 September 1954, Declassified Report, quoted in William Leary (Ed.), *The Central Intelligence Agency: History and Documents*, University of Alabama Press, 1984.

[34] The authors of the report conclude that following the dissolution of the Soviet Union, most of the intelligence communities assessments were vindicated, "…at least in the areas in which it had spent the largest part of its efforts, the Soviet bloc's military equipment, capabilities and order of battle". Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, p.15. Italics added by author.

[35] Matthew Grant, Introduction: The Cold War and British National Interest, in Matthew Grant (Ed.), *The British way in cold warfare: intelligence, diplomacy and the bomb, 1945-1975*, Continuum, London, 2009, pp.1-14, p.8. Italics added by author.

[36] Michael Goodman (2007): The Dog That Didn't Bark: The Joint Intelligence Committee and Warning of Aggression, Cold War History, 7:4, 529-551, Pp.531-532.

[37] Stephen Robert Twigge, Graham Macklin, Edward Hampshire, *British Intelligence: Secrets, Spies and Sources*, The National Archives, London, 2008, p.14. Italics added by author.

intelligence during the Cold War, with scientific and technical intelligence playing key roles".[38] Focussing on British and the broader allied intelligence assessments, Loch Johnson provides an insight into the central importance of the concept of intentions and capabilities in assessing the Soviet threat. Johnson writes that:

> How far, and in what way, the United Kingdom's national survival was at risk during the Cold War remains an intriguing question for those exploring the role of intelligence in national security. How far, and in what ways, the Soviet Union threatened that survival requires careful scrutiny of not only British (and other allied assessments) but of course the Soviet *capabilities* and *intentions* that were the focus of the estimates. Attempts to reach judgments on the veracity of British assessments therefore remain contingent on the availability of information about Soviet *intentions* and *capabilities*.[39]

No doubt the sharing of intelligence analysis and reporting between the UK and US, often including entire reports, would also have reinforced continued framing of state threat in terms of intentions and capabilities. As Aldrich notes "[m]any of the more substantial JIC reports – typically London's large annual survey of Soviet intentions and capabilities,

---

[38] *Ibid.*, p.12. Italics added by author. It should also be noted that by the mid-1960s, JIC was increasingly concerned over the potential for accidental war or entering the war through miscalculation, as noted by Peter Hennessey. According to Hennessey, "[t]he immense latent power of each other's nuclear arsenals, and their state of readiness, had, by this stage, added new levels to old anxieties. It was the danger of 'accident and miscalculation' which now represented the great preoccupation of British intelligence. In that short hiatus between the Berlin and Cuban crises, the JIC concluded:

> Even when there is no particular political tension each side now has a proportion of its nuclear strike forces constantly at immediate alert. There must be a risk, however remote that by pure mechanical or electrical accident one of the missiles might be launched; or that through misunderstanding one might be launched by human agency within this being the intention of the Government concerned concerned…"

Further "…setting aside the notions of war-by-accident, the JIC, on the assumption 'that the Soviet leaders act rationally', saw the possibility of war-through-miscalculation erupting due to the lighting of three possible fuses:

(a) the Soviet Union or the West in some critical or tense situation were to make a false appreciation of what was considered by the other side to be intolerable; or
(b) the Soviet Union or the West were to believe wrongly that the other had weakened in its determination to use nuclear weapons if pressed too far; or
(c) either side were to fail accurately to foresee the consequences of the policies being pursued by a third party with which it was associated."

Peter Hennessey, *The Secret State: Whitehall and the Cold* War, Penguin Books, London, 2003, p.38 [quoting from PRO, CAB 158/44 JIC (62) 10, 'The Likelihood of War with the Soviet Union up to 1966', 9 February 1962.

[39] Len Scott, British Strategic Intelligence and the Cold War, in Loch Johnson (Ed.), *The Oxford handbook of national security intelligence*, Oxford University Press, Oxford, 2010, p.142. Italics added by author.

running to seventy pages, were sent verbatim to Washington".[40] Similarly, Len Scott highlights this sharing of formal assessments between British and American intelligence agencies. Scott highlights that "[i]n general, the British and American intelligence services shared sources and the intelligence communities shared assessments. The British saw US National Intelligence Estimates (NIEs) and Special Intelligence National Intelligence Estimates (SNIEs). The British were shown JIC estimates".[41]

Whilst discussion of intentions and capabilities were a focus of Australian intelligence assessments during the 1950s, the reliance on these parameters was not nearly as prominent as in the US and British intelligence assessments.[42] Stephan Fruhling makes the argument that threat, within the Australian context, "…often meant the contribution to allied action in support of wider interests, rather than a direct possibility of harm to Australia itself".[43] Nevertheless, by the 1970s, the conventional model of threat featured prominently in Australian Defence white papers as well as strategic threat assessments. This is apparent in the *Strategic Basis of Australian Defence Policy 1971* which concluded that "[i]t is very unlikely that any Indonesian Government in this decade would develop a *capability* or *intention* to mount a serious and sustained attack on the Australian mainland. We could expect warning over a period of years of any change of Indonesia's intention or capability".[44] Given such a widespread use and acceptance of this approach, it is little

[40] Richard Aldrich, *The Hidden Hand: Britain, America and Cold War Secret Intelligence*, John Murray, London, 2001, p.85.
[41] Len Scott, British Strategic Intelligence and the Cold War, in Loch Johnson (Ed.), *The Oxford handbook of national security intelligence*, Oxford University Press, Oxford, 2010, p.149.
[42] For example, refer to Defence Committee, *A Strategic Basis of Australian Defence Policy*, Defence Committee Report, 8 January 1953; Joint Intelligence Committee, *Intelligence Aspects of the Strategic Basis for Australian Defence Policy*, JIC (M) 35 August 1956; and Defence Committee, *Strategic Basis of Australian Defence Policy*, December 1958.
[43] Stephan Frühling, *A History of Australian Strategic Policy Since 1945*, Defence Publishing Service, Canberra, 2009, p.2.
[44] Defence Committee, *Strategic Basis of Australian Defence Policy*, March 1971, in Stephan Frühling, *A History of Australian Strategic Policy Since 1945*, Defence Publishing Service, Canberra, 2009, p.427. Italics

surprise that some have claimed that intelligence is only about adversary's intentions or capabilities. For example, writing as the Cold War was ending, Michael Handel in his book *War, Strategy and Intelligence* makes the statement that "[a]ll information gathered by intelligence concerns either the adversary's *intentions* or his *capabilities*".[45]

Following the end of the Cold War, governments and intelligence agencies have continued to use the conventional model to assess state-based threats. This is evident through a brief examination of publicly released intelligence assessments and strategic documents. In the United States, evidence of the continuing application of these parameters for assessing threat is apparent in a number of official publications, including the 2007 National Intelligence Estimate, *Iran: Nuclear Intentions and Capabilities*.[46] In Australia, the Government's 2009 Defence White Paper framed the purpose of Defence intelligence as providing "…insights into the strategic posture, policy, *intent* and military *capabilities* and proliferation activities of countries relevant to Australia's national security".[47] Similarly, the British Government's 2009 *National Security Strategy* concludes that "…in the foreseeable future, there will remain no state with the *intent* and *capability* to threaten the independence, integrity and self-government of the UK mainland".[48] It is, therefore, evident that government agencies within the UK, United States and Australia continue to employ Singer's concept of threat for assessing conventional threats from states.

---

added by author. For additional examples, refer to the Commonwealth Government, *Australian Defence*, November 1976 (1976 Australian Defence White Paper); as well as the Defence Committee *Strategic Basis of Australian Defence Policy*, 5 March 1971; Defence Committee *Strategic Basis of Australian Defence Policy*, 1 June 1973 and Defence Committee *Strategic Basis of Australian Defence Policy*, 3 October 1975.

[45] Michael Handel, *War, Strategy, and Intelligence*, Frank Cass and Company Limited, Totowa, 1989, p.239. Italics as per Handel's text.

[46] National Intelligence Council, *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007.

[47] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p.102. Italics added by author.

[48] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, p.41. Italics added by author.

Indeed, the dominance of this approach is highlighted by Glen Segell, who argues that the trends and patterns approach, which "…can be equated with and referred to as the analysis of intent and capability", remains the most significant methodology for state-based conflict, diplomatic intelligence, the primary methodology for military intelligence analysis.[49] According to Segell, the continued reliance on this approach is based on its success and simplicity in training and coping with staff turnover in intelligence agencies.[50] The use of this method has enabled new staff to quickly focus on gathering data and conducting analysis using this well-established technique.[51] If the immediate training and indoctrination intelligence analysts receive involves a concept of intelligence as the *analysis of intent and capability,* and of threat as intent and capability, then it is little wonder that the model has largely avoided attracting deep and detailed critique.

1.3 The Challenge of Non-State Actors and the Expectations of Intelligence

> The end of the Cold War brought about not only the end of a relatively stable bipolar world order but also the end of the boundedness of threats. The components of the post-Cold War security paradigm are more diverse and diffuse than were their counterparts during the Cold War.
>
> Myriam Dunn Cavelty and Victor Mauer[52]

[49] Glen Segell, Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004, *International Journal of Intelligence and Counterintelligence*, Vol.18, No.2, pp.221-238, p.224.
[50] *Ibid.*, pp.224-225.
[51] *Ibid.*, pp.224-225.
[52] Myriam Cavelty and Victor Mauer, Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence, *Security Dialogue*, Vol. 40, No.2, April 2009, pp.123-144, p.127.

Singer's description of a bi-polar, state-based security context is reflected in the views held by intelligence analysts, officials and decision-makers of the period. As evident in *NSC-68: United States Objectives and Programs for National Security*, the bi-polar perspective provided a frame through which to view power within international relations. The assessment argues that "…the defeat of Germany and Japan and the decline of the British and French Empires have interacted with the development of the United States and the Soviet Union in such a way that power increasingly gravitated to these two centres".[53] The Cold War provided a period of bipolarity within which Soviet Union and the United States as the two major nuclear superpowers provided a balance of power and a framework within which international affairs were conducted.[54] This bi-polarity provided a frame through which analysts were able to assess and analyse threats, with threatening behaviour of states and regional sub-conflicts evaluated within the context of how Moscow and Washington might perceive these and respond. The corollary was that state and non-state actors were also conscious of the Cold War framework and the potential for involvement or responses from either or both sides in any threatening actions that they planned on undertaking.

With the end of the Cold War, and the loss of this bi-polar, state-based system, concepts of security have shifted away from a highly militarized confrontation between fixed opponents to concern over difficult-to-identify non-state threats.[55] Consequently, an adequate sense of the contemporary international environment cannot be achieved solely by considering state-based threats.[56] Before the 11 September 2001 attacks, the concept of

[53] National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950, accessed 31 October 2007 at: www.fas.org/irp/offdocs/nsc-hst/nsc-68-1.htm.
[54] Rodney Coombe, *Security in the post–Cold War Asia–Pacific*, Australian Defence College, Monograph Series, No. 2, 2003, p.6.
[55] David Kahn, The Rise of Intelligence, *Foreign Affairs*, Sep/Oct2006, Vol. 85 Issue 5, pp.125-134.
[56] Peter Layton, Redefining Warfare, *Royal United Services Institute Journal*, Feb 2007, Vol 152, No.1, pp.34-41, p.37.

strategic threats had principally been applied to states and their militaries.[57] With successful mass-casualty attacks against civilians, there is an argument that non-state actors have become strategic threats, with the concept of "strategic terrorism" being raised immediately after the attacks of September 2001. Bruce Berkowitz makes the argument that "[t]o be sure, governments, political organizations, social malcontents, revolutionaries, and oppressed ethnic minorities have employed terrorism in the past. Some terrorist organizations have even carried out attacks over long distances (e.g. the IRA bombed London in the 1980s, Chechens bombed Moscow in the mid-1990s). But bin Laden was the first to use strategic terrorism in a successful large-scale military strike against a superpower – and to devastating effect".[58] Further, it has been suggested that the characteristics of state and non-state actors are becoming increasingly similar in terms of weapons, lethality and technological sophistication.[59] Globalisation and the movement of people and technology have empowered non-state actors with the tools to enact massive physical and psychological destruction which have impacted political, economic and global stability.[60] As Elke Krahmann observes, "[n]on-state threats and actors have become key factors in contemporary security".[61] This "more complex and dangerous" security

[57] MacEachin argues that prior to September 11, "…the concept of a 'strategic threat' had been wedded to state actors and military forces. Insofar as this concept had been applied to the hierarchy of nonstate threats, it had focused mainly on those that were—or were believed to be — state-supported quasi surrogates." Douglas MacEachin, Analysis and Estimates: Professional Practices in Intelligence Production, in eds. Jennifer Sims and Burton Gerber, *Transforming US Intelligence*, Georgetown University Press, Washington, D.C., 2005, p.125.

[58] Bruce Berkowitz, Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, pp.289-300, p.289.

[59] According to the authors of *Complex Warfighting*, "[n]on-state actors have always been part of warfare. However, the characteristics of state and non-state actors are becoming increasingly similar. Non-state actors now operate sophisticated weapons systems, may control territories and populations, and possess lethality and technological sophistication that was once the preserve of states and their regular armed forces." Department of Defence, *Complex Warfighting*, Commonwealth of Australia, Canberra, April 2004, p.8 available at:
http://www.defence.gov.au/army/lwsc/Publications/complex_warfighting.pdf accessed on 02 September 2006.

[60] Edward Waltz, *Knowledge Management in the Intelligence Enterprise*, Artech House, Boston, 2003, p.48.

[61] Elke Krahmann, From State to Non-State Actors: The Emergence of Security Governance, in ed. Elke Krahmann, *New Threats and New Actors in International Security*, Palgrave MacMillan, New York, 2005,

environment[62], with a mixture of both state and non-state threats, presents as a greater conceptual challenge for analysts. According to Colin Wastell *et al,* "[s]ince the end of the Cold War there has been a disaggregation of old alliances and an emergence of non-state based actors and groups. The world is arguably much more complex and fragmented. …This new context places demands on analysts to think in new categories".[63]

One of the most notable observations of this shift from a bi-polar, state-based context to a more complex and nebulous context of threat was the testimony by the CIA Director, James Woolsey, to the US House of Representatives Committee on National Security. Woolsey testified that "…it is as if we were struggling with a large dragon for 45 years, killed it, and then found ourselves in a jungle full of poisonous snakes - and the snakes are much harder to keep track of than the dragon ever was".[64] The "Soviet deprivation" of the post-Cold War and the focus on "…increasingly fleeting, elusive, low-profile, and security-conscious…" non-state threats present a different type of problem for identifying and assessing threat.[65] Indeed, in contrast to the bi-polar context within which Singer was writing, the contemporary security context has been described as one of "strategic heterogeneity".[66] This thesis does not argue that state-based threats are no longer a primary concern for intelligence analysts and decision-makers. Clearly, the identification and assessment of state-based threats remain a strategic priority for governments and their

---

p.1. It is important to acknowledge that mass-killing power for states have also increased with the increased development of technology, including nuclear, biological and chemical weaponry.

[62] George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, p.13.

[63] Colin Wastell, Graeme Clark, and Piers Duncan, Effective Intelligence Analysis: The Human Dimension, *Journal of Policing, Intelligence and Counter Terrorism*, Vol.1, October 2006, pp.36-52, p.37-38.

[64] James Woolsey, Testimony, 12 February 1998, US House of Representatives Committee on National Security accessed at:
http://www.globalsecurity.org/intell/library/congress/1998_hr/h980212w.htm on 31 March 2008.

[65] James Hansen, US Intelligence Confronts the Future, *International Journal of Intelligence and CounterIntelligence*, Vol.17, 2004, pp.673-709, p.691.

[66] Rod Lyon, Six Challenges, in Coral Bell et. al., *Scoping Studies: New thinking on security*, Australian Strategic Policy Institute, Barton, 2004, p.15.

intelligence agencies.[67] The point is that, in addition to state-based threats, identifying and assessing non-state actors has *also* become a strategic priority for intelligence agencies. In 2007, Jonathan Evans, Director General of the United Kingdom's Security Service (MI5), described the terrorist threat as "…the most immediate and acute peacetime threat in the 98-year history of my Service".[68]

The importance given to intelligence in dealing with non-state threat actors is evident in governments' actions and publications as well as the establishment of new government departments and agencies. As a direct consequence of the September 2001 attacks, the United States Government established the Department of Homeland Security (DHS), bringing together programs and staff from over twenty existing government departments to create the DHS.[69] The original mission of the DHS was to "[p]revent terrorist attacks within the United States; reduce America's vulnerability to terrorism; and minimize the damage and recover from attacks that do occur".[70] In 2003, the British Government established the Joint Terrorism Analysis Centre (JTAC) to provide analysis and assessments of "…intelligence relating to international terrorism, at home and overseas".[71] JTAC is an independent intelligence agency, drawing staff from sixteen government

[67] In terms of the ongoing priority given to identifying state-based threats refer to: Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008; Cabinet Office, *The National Strategy of the United Kingdom: Security in an interdependent world*, The Stationery Office, London, March 2008; United States Department of Defense, *Quadrennial Defense Review Report*, Washinton, D.C., February 2010.

[68] Jonathan Evans, *MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust*, 5 November 2007, accessed at: www.cfr.org/publication/14789/mi5_director_generals_speech_on_intelligence_counterterrorism_and_trust_html on 9 May 2009.

[69] Department of Homeland Security, *History: Who Became Part of the Department?*, accessed on 23 February 2011 at: http://www.dhs.gov/xabout/history/editorial_0133.shtm

[70] George W. Bush, *The Department of Homeland Security*, The White House, Washington, D.C., June 2002, p.8.

[71] Security Service, *Joint Terrorism Analysis Centre*, accessed on 23 February 2011 at: https://www.mi5.gov.uk/output/joint-terrorism-analysis-centre.html

departments and intelligence agencies.[72] In 2004, following the 2002 Bali bombings, the Australian Government created the National Threat Assessment Centre (NTAC) to provide threat assessments of "…terrorism and politically motivated violence" to Australian citizens and interests within Australia and overseas.[73]

Government publications in the United States, Australia and Great Britain released in the months after the 11 September 2001, 2002 Bali bombings and 2005 London bombings reflected a consensus that intelligence is critical in preventing mass-casualty attacks. The concept of intelligence as a "first line of defence" against these types of attacks appears in the United States' 2002 *National Security Strategy*[74] and the Australian Government's publication *Protecting Australia Against Terrorism.*[75] In *Countering International Terrorism: The United Kingdom's Strategy*, intelligence is seen as "vital to defeating terrorism".[76] Perceptions of intelligence as both defensive and offensive are also reflected in the intelligence literature. For example, Amy Zegart argues that during the Cold War, with a more easily detectable enemy, "…the first and last line of defense was military power. Now it is intelligence".[77] Borgu argues that intelligence is both "the front line

[72] *Ibid.*
[73] According to the Department of Foreign Affairs and Trade, the NTAC "comprehensively monitors and analyses all intelligence and information relating to terrorism available to the Australian Government". The agency also "prepares assessments of the likelihood and probable nature of terrorism and other acts of politically motivated violence against Australia, Australian citizens here and abroad and Australian interests overseas". In addition to staff from the Australian Security Intelligence Organisation, the NTAC also has staff from across Australia's security and intelligence agencies, including the Australian Federal Police, the Australian Secret Intelligence Service, the Defence Intelligence Organisation, the Department of Foreign Affairs and Trade, the Department of Transport and Regional Services and the Office of National Assessments. Department of Foreign Affairs and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004, p.100.
[74] George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, p.30.
[75] The Department of Prime Minister and Cabinet, *Protecting Australia Against Terrorism*, Commonwealth of Australia, Canberra, 2004, p.20.
[76] United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.l6.
[77] Amy Zegart, Cloaks, Daggers, and Ivory Towers: Why Academics Don't Study US Intelligence, in ed. Loch Johnson, *Strategic Intelligence 1: Understanding the Hidden Side of Government*, Praeger Security

defence and offence against terrorism".[78] The 9-11 Commission goes one step further, arguing that "[n]ot only does good intelligence win wars, but the best intelligence enables us to prevent them from happening altogether".[79]

Beyond the government and agencies publications, intelligence literature and formal inquiries, there is also a greater public awareness and expectation of what intelligence agencies can and should provide.[80] This has come about for a number of reasons. One reason is a result of the shock experienced by the general public at witnessing actual attacks or their aftermath.[81] Indeed, recent mass-casualty attacks indicate that at least some groups consider civilians to be legitimate targets acting upon a belief that "there are no innocents".[82] Consequently, if civilians are themselves the potential target of any attack, the general public may perceive a vested interest in the work of intelligence analysts. The conduct of mass-casualty attacks against civilians does present a critical shift from previous attacks by non-state actors. Writing on the 1993 World Trade Centre attacks,

---

International, Westport, 2007, p.21.

[78] Aldo Borgu, *Understanding Terrorism:20 basic facts*, Australian Strategic Policy Institute, Barton, September 2004, pp.9-10.

[79] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004, p.420.

[80] Sir David Ormand argues that "[t]here are public expectations that government will be able to provide threat warnings and advice on how risks to individuals and businesses can be minimised both at home and when travelling or working overseas. And when things happen that affect the citizen anywhere in the world, such as the tragic terrorist bombing of a tourist bar in Bali, the intelligence agencies should not be surprised when public opinion demands inquiries by oversight committees into their work, into what they knew and what they might have been expected to know that could have allowed the attack to occur". Sir David Ormand, *The National Security Strategy: Implications for the UK intelligence community*, Institute for Public Policy Research, Discussion Paper, February 2009, p.5.

[81] Rolington observes that "…the world watched in real time as the second plane crashed into the tower in New York on 9/11. This had never happened so dramatically before and it has changed people's relationship with dramatic events. The first moment most government officials even in the US became aware of 9/11 was from a CNN live broadcast. Such processes are altering people's perception of news but also politics and policy-makers' response to events". Alfred Rolington, Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.738-759, p.751.

[82] Author's interview with Richards Heuer March 2007. The idea of "no innocents" is also applicable to nuclear warfare (and even conventional warfare in the case of bombings of cities) as nuclear weapons are also mass-casualty weapons that, if employed, clearly would not distinguish between military personnel and civilians.

Hoffman argues that the attempted mass-casualty attacks represented a significant change from previous terrorist attacks. Hoffman observes that "…there is no evidence that the secular or 'professional' terrorists of the past - the persons once considered to be the world's arch-terrorists, such as the Carloses, Abu Nidals and Abul Abbases - ever contemplated, much less attempted, the complete destruction of a high-rise office building packed with people".[83] Similarly, Borgu argues that "…the mass-terrorism threat we face today is very different from the siege-hostage incidents of the 1970s …Mass-terrorism aims to inflict maximum casualties as quickly as possible, with no thought of negotiation and no time for protracted response once an incident has begun".[84] Laqueur highlights that "[c]ontemporary terrorism has increasingly become indiscriminate in the choice of its victims", shifting its aim from propaganda to maximum destruction.[85] Indeed, at least one commentator has argued that it is actual and potential mass-killing of civilians that represents the only innovative change in contemporary terrorism.[86] Yet, the deliberate killing of civilians has been enough to lift the priority for analysts in identifying actual and potential non-state threats. Finally, the actions of governments themselves have also increased public awareness and expectations of intelligence. Governments' use of intelligence analysis to inform and shape public perceptions of threats has increased public awareness and interest in intelligence.[87] Nevertheless, despite how important intelligence

[83] Bruce Hoffman, *Inside Terrorism*, Columbia University Press, New York, 1998, p.204.
[84] Aldo Borgu, *Beyond Bali: ASPI's Strategic Assessment 2002*, Australian Strategic Policy Institute, 2002, p.16.
[85] Walter Laqueur, *No End to War: Terrorism in the Twenty-First Century*, The Continuum International Publishing Group Inc, 2003, p.9.
[86] Zimmerman argues that "…the combination of the technology to inflict mass casualties measured in the hundreds of thousands, or even in the millions, on the one hand, and the increasing likelihood of the acquisition of the means to bring about such massive destruction of life by sub-state actors on the other constitutes the only evidently innovative aspect in the development of contemporary terrorism". Doron Zimmermann, Terrorism Transformed: The "New Terrorism," Impact Scalability, and the Dynamic of Reciprocal Threat Perception, *The Quarterly Journal*, Vol. 3, No. 1, March 2004, pp.19-39, p.25.
[87] In considering the UK's experience Christopher Andrew makes this argument, observing that "…more intelligence and intelligence related material than ever before enters the public domain". The same conclusion is also applicable to recent experience within the United States and Australia. See, Christopher

has come to be perceived, Singer's model has largely been adopted uncritically as the basis for assessing threats within this new security context.

1.4 The Persistence of Singer's Model: Assessing Non-State Threats

A review of recent government and intelligence publications illustrates that Singer's model is being used as the primary approach for assessing non-state threats. Threat levels published by intelligence agencies within Australia and the United Kingdom highlight the extent to which assessments of non-state threats have adopted Singer's concept.[88] Further, the adoption of this approach by United States agencies assessing non-state threats is also apparent. It is worth highlighting a number of examples to demonstrate the penetration of the concept.

In the United Kingdom, threat levels currently used by the Secret Service and the Joint Terrorism Analysis Centre (JTAC) to assess terrorist threat are based on "…current intelligence, recent events and what is known about terrorist *intentions* and *capabilities*".[89]

Andrew, Intelligence, International Relations and 'Under-theorisation', *Intelligence and National Security*, Vol.19, No.2, Summer 2004, pp.170-184, p.170.

[88] Refer to: Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006, p.20; and Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A, accessed at:
www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub02.pdf
At the time of writing, the Government of the United States has not publicly released the criteria used to establish national terrorism threat levels (Homeland Security Advisory System). The Threat Level System is described at: www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

[89] United Kingdom Government, *Threat Levels: The System to Assess the Threat from International Terrorism*, The Stationery Office, London, July 2006, p.2. The wording of the threat levels can be found in the report into the 2005 London bombings, Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006. It is evident that the JTAC, established in 2003, has adopted the concept of threat and applied this to assessing the terrorist threats. According to the United Kingdom publication *National Intelligence Machinery* "JTAC has become widely recognised as an authoritative and effective mechanism for analysing all-source intelligence on the activities, *intentions* and *capabilities* of international terrorists who may threaten UK and allied interests worldwide. It sets threat levels and issues timely threat warnings (relating to international terrorism) as well as providing more in-depth reports on trends, terrorist networks and capabilities". Cabinet

In describing the scale of terrorist threat, the UK's Intelligence and Security Committee's 2006-2007 Annual Report states that there were "…approximately 200 extremist networks under investigation, some of which have both the *intent* and *capability* to carry out attacks against the UK or UK interests overseas".[90] The UK Government publication *Countering International Terrorism: The United Kingdom's Strategy* outlines the use of information and intelligence to "…identify terrorist networks, including their membership, *intentions*, and means of operation".[91] Before this, the British Cabinet Office released *The United Kingdom and The Campaign against International Terrorism.* They argued that the threat from Al Qa'ida and extremist groups remained as "…it is clear they retain the *capability* and *intention* to mount attacks".[92] Immediately following the 11 September 2001 attacks in the United States, the British government released two assessments on the threat from Osama bin Ladin and Al Qa'ida employing largely identical parameters (*resources* and *will*) to describe the threat from the group.[93] Similarly, the United Kingdom's 2003 *Defence White Paper* defines the threat from Al Qa'ida in terms of retaining "the *intent* and *capability* to pose a direct threat to the UK and to British citizens".[94]

In the United States, the National Intelligence Estimate *The Terrorist Threat to the US Homeland* assesses that the main terrorist threats come from "Islamic terrorist groups and cells, especially al-Qa'ida, driven by their undiminished *intent* to attack the Homeland"

Office, *National Intelligence Machinery*, The Stationery Office, London, November 2006, p.16. Italics added by author.

[90] Intelligence and Security Committee, *Intelligence and Security Committee: Annual Report: 2006-2007*, 2007, p.3. Italics added by author.

[91] United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.16. Italics added by author.

[92] Cabinet Office, *The United Kingdom And The Campaign against International Terrorism: Progress Report*, September 2002, p.32. Italics added by author.

[93] 10 Downing Street, *Responsibility for the Terrorist Atrocities in the United States: 11 September 2001*, 4 October 2001; and 10 Downing Street, *Responsibility for the Terrorist Atrocities in the United States: 11 September 2001- An Updated Account*, 14 October 2001. Italics added by author.

[94] Ministry of Defence, *Delivering Security in a Changing World*, The Stationery Office, London, 2003, p.4. Italics added by author.

and continued effort "…to adapt and improve their *capabilities*".[95] The United States' 2006 *National Strategy for Combating Terrorism* outlines concerns over the threat of terrorist groups using weapons of mass destruction (WMD) and the importance of identifying "terrorists' *intentions*, *capabilities*, and plans to develop or acquire WMD".[96] The *National Intelligence Strategy of the United States of America* argues the need for "new methodologies" when dealing with non-state threats, but frames these within the conventional approach of "analysing the *capabilities* and *intentions*".[97] The United States' *National Strategy for Homeland Security*, similarly defines threat in terms of *will* and *capability*, noting that "international terrorist organizations, as well as domestic terrorist groups, possess the *will* and *capability* to attack the United States".[98] Finally, the 2008 *Defense Intelligence Strategy* highlights the desire to understand "the *capabilities* and *intentions* of state and non-state actors" in relation to developing WMD.[99]

In Australia, the Government's 2010 *Counter-Terrorism White Paper* argues that "Australia's response to terrorism is driven by our understanding of current and emerging threats and the *intent*, *capability* and operational methods of terrorist groups".[100] The Defence Intelligence Organisation (DIO) mandate details the agency's responsibility to provide "assessments of the *capabilities*, *methods* and *intent* of foreign non-state actors

[95] National Intelligence Council, *The Terrorist Threat to the US Homeland*, Office of the Director of National Intelligence, Washington, D.C., July 2007. Italics added by author.
[96] National Security Council, *National Strategy for Combating Terrorism*, Washington, D.C., September 2006, p.14. Italics added by author. WMD is generally associated with chemical, biological, radiological and nuclear (CBRN) weapons.
[97] Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005, p.9. Italics added by author.
[98] Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.vii. Italics added by author.
[99] Office of the Under Secretary of Defense for Intelligence, *Defense Intelligence Strategy*, Washington, D.C., 2008, p.16. Italics added by author.
[100] Department of the Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia, Protecting Our Community*, Commonwealth Government of Australia, Canberra, 2010, p.28. Italics added by author.

which pose a potential or actual threat to Australia's interests".[101] The *2009 Defence White Paper* frames the role of intelligence as providing "insights into the *actions, capabilities, motives* and *intent* of foreign non-state actors".[102] The threat levels used by the Australian Security Intelligence Organisation (ASIO) similarly based assessments of threat on assessments of intentions and capabilities.[103] For example, ASIO's *Report to Parliament 2008-2009* assesses that "the Middle East, South Asia and now East Africa are the primary sources of *motivation* and *capability* for extremists in Australia".[104] A year earlier, ASIO had reported threats from Indonesian Islamic extremists in terms of "ongoing terrorist *intent* and *capability*".[105] Interestingly, in *Transnational Terrorism: The Threat to Australia*, Australia's Department of Foreign Affairs and Trade (neither an intelligence nor a defence agency) adopted these parameters in arguing that the severity of the threat is based upon "…the strong *intention* and *capability* of terrorist organisations to strike".[106]

In addition to its near-universal uptake within intelligence agencies, the application of Singer's model to non-state actors is largely accepted within the wider intelligence and security literature. For example, Boaz Ganor argues that "…terrorism is a combination of two factors - *motivation* to attack and the operational *capability* to do so".[107] Brian Jackson

---

[101] Commonwealth Government of Australia, *The Australian Intelligence Community: Agencies, functions, accountability and oversight*, Commonwealth of Australia, Canberra, 2006, p.10. Italics added by author.
[102] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p.102. Italics added by author.
[103] Refer to Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A, accessed at: www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub02.pdf
[104] Australian Security Intelligence Organisation, *ASIO Report to Parliament 2008-09*, Commonwealth of Australia, Canberrra, 2009, p.xv. Italics added by author. The term *motivation* is often used interchangeably with the term intention.
[105] Australian Security Intelligence Organisation, *ASIO Report to Parliament 2007-08*, Commonwealth of Australia, Canberrra, 2008, p.5. Italics added by author.
[106] Department of Foreign Affairs and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004, p.49. Italics added by author.
[107] Boaz Ganor, The Changing Threat of International Terrorism, *The Sydney Papers*, Winter 2002, pp.43-51, p.47. Italics added by author.

argues that "[u]nderstanding a terrorist group's *intentions* and *capabilities*, the types of operations it may attempt, and its chances of being successful when it stages an operation is critical for effective efforts to combat terrorism".[108] Michael Ronczkowski makes a similar observation, noting that "[t]hreat assessment approaches involve many factors, but three of the most common are a terrorist group's *intentions*, *past activities*, and *capabilities*. These factors are detected throughout the analytical and investigative processes and should be applied when developing threat assessments".[109] Edite et al. argue that "…terrorism generates difficulties for states, as military planners may not have sufficient information regarding the *intentions* and *capabilities* of terrorists".[110] Evans et al. argue that, whilst being aware of Al Qa'ida for a long period, what is lacking "…is some knowledge about their *capability* and a great deal of knowledge about their *intent*".[111] Methodological approaches to analysing non-state threats have similarly adopted this model. For example, Hank Prunkun in *Handbook of Scientific Methods of Inquiry for Intelligence Analysis* identifies the conventional model as an analytical technique for use in counterterrorism.[112] Accordingly, it appears that commentators' conceptualisations of non-state threat are consistently based on Singer's model.

Investigators involved in reviewing the performance of intelligence agencies have also regularly accepted and employed this model of threat. For example, the 2004 *Report into*

[108] Brian Jackson et al., *Aptitude for Destruction Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, RAND Corporation, Santa Monica, 2005, p.3.
[109] Michael Ronczkowski, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, CRC Press, Boca Raton, 2004, p.109. Italics added by author.
[110] T. Paul, The National Security State and Global Terrorism: Why the State Is Not Prepared for the New Kind of War, in Ersel Aydinli and James Rosenau (Eds.), *Globilization, Security and the Nation-State: Paradigms in Transition*, State University of New York Press, Albany, 2005, p.56. Italics added by author.
[111] Michael Evans, Alan Ryan and Russell Parkin (Eds.), *Future Armies, Future Challenges: Land warfare in the information age*, Allen & Unwin, 2004, p.172. Italics added by author.
[112] Hank Prunkun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Lanham, 2010, Chapter 11, pp.162-179.

Australian Intelligence Agencies (the Flood Report) applies the criteria of capabilities and intentions in assessing the performance of intelligence agencies. Philip Flood concludes that "Australian intelligence agencies should have known more before December 2001 about JI [Jemaah Islamiyah] as a group developing terrorist *capabilities* and *intentions*".[113] Similarly in the United States, *The 9-11 Commission Report* recommended the establishment of a National Counter Terrorist Committee (NCTC) that "…should develop net assessments (comparing enemy *capabilities* and *intentions* against US defenses and countermeasures)".[114] In the United Kingdom, the *Review of Intelligence on Weapons of Mass Destruction* (Butler Review) analysed the performance of British intelligence agencies assessments of Osama bin Ladin and Saddam Hussein's capabilities and intentions.[115] Thus, opportunities to formally critique the widespread acceptance of the conventional model of threat have been lost. Instead, investigations and inquires have often reinforced the concept of threat by adopting it as a measure against which to assess the performance of intelligence agencies and analysts. The final result of this is that, inasmuch as reviewers and examiners have uncritically adopted the model of threat used by intelligence agencies, they have limited their reports to a very narrow assessment of performance against established concepts. The question of the effectiveness of the concepts themselves has remained unexamined. This actually hinders the development of intelligence analysis as a field of research as those within the field have provided the criteria against which it is assessed rather than being subjected to critique against externally-developed criteria.

---

[113] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.41. Italics added by author.
[114] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004, p.404. Italics added by author.
[115] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004.

One argument could be that the successful identification, disruption and prosecution of a number of groups planning mass-casualty attacks is evidence that the conventional approach *is* effective in identifying and assessing non-state threats. Based upon this argument, any failure to identify groups planning attacks would, therefore be evidence that the conventional approach is *not* effective. Perhaps a better way of looking at the problem is considering G. Box's argument that "all models are wrong but some are useful".[116] Any conceptual model of threat attempts to simplify what is an inherently (and arguably irreducibly) complex phenomenon. Acknowledging such a simplification, the question is then the extent to which such models aid or hinder understanding of threat and, importantly, identifying the assumptions underpinning the model. The purpose of this study is to identify the *limitations* of Singer's model when applied to non-state actors, rather than argue over whether the model is right or wrong. The model itself is useful insofar as its limitations are identified and articulated. Without identifying these limitations, assessments using the model might appear more credible or reliable than would actually be warranted. The rationale for identifying limitations is succinctly captured by Lord Butler in the *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors.* Butler observes that "[i]ntelligence merely provides techniques for improving the basis of knowledge. As with other techniques, it can be a dangerous tool if its limitations are not recognised by those who seek to use it".[117]

[116] G.E.P. Box, *Robustness in the Strategy of Scientific Model Building*, in R.L. Launer and G.N. Wilkinson (Eds.) Robustness in Statistics: Proceedings of a Workshop. New York: Academic Press, 1979.

[117] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.14-15.

1.5 Intelligence Analysis: An Under-Theorised Field of Research

Christopher Andrew makes the argument that intelligence remains an "under-theorised" field of research. According to Andrew, the lack of inclusion of intelligence in international relations, particularly in analysis of the Cold War and dynamics of authoritarian states, presents as a problem for both academic research and public discussion on intelligence. Andrew's identifies two reasons why this has occurred: difficulty in accessing the intelligence archive; and cognitive dissonance in adapting now available information on intelligence into conventional ideas in international relations.[118] This idea of under-theorised field of research can also be made to the more specific area of intelligence analysis. Indeed, despite increased focus on preventing major attacks such as those that occurred in New York and Washington (2001), Bali (2002 and 2005) and London (2005), and the attention given to intelligence by governments and the media, there is a perception or acceptance that intelligence, and intelligence analysis particularly, remains an "under-theorised" field of research. For example, despite the unprecedented time and resources invested into the 9-11 Commission, Schmitt highlights that the Commission's final report actually has very little to say on intelligence *analysis* per se.[119] This is not to suggest that important work has not been undertaken within the field of intelligence analysis, but perhaps reflects its ongoing development as a relatively new academic field of research.

Michael Goodman makes the observation that "[w]hilst intelligence is not a new

[118] Christopher Andrew, Intelligence, International Relations and 'Under-theorisation', *Intelligence and National Security*, Vol.19, No.2, Summer 2004, pp.170-184, p.181.
[119] Schmitt makes the argument that, despite being nearly 500 pages in length, only six pages of the 9/11 Commission report are directly concerned with analysis. Gary Schmitt, Truth to Power? Rethinking Intelligence Analysis, in ed. Peter Berkowitz, *The Future of American Intelligence*, Hoover Institution Press, Stanford, 2005, p.41.

phenomenon, the academic study of it is".[120] Coinciding with the recent development of the academic study of intelligence has been the research and development of the more specific field of intelligence analysis, including its theoretical, methodological and practical aspects.[121] Nevertheless, the intelligence as a field of research remains a *maturing* one, still lacking an accepted definition of what *intelligence* actually is.[122] Intelligence can be described as both a process and an end-product[123], with efforts to articulate the process of intelligence perhaps best captured in the concept of an "intelligence cycle". The intelligence cycle, often displayed visually, consists of five steps: planning and direction; collection; processing; analysis; and dissemination.[124] For the purposes of the reader familiar with the intelligence cycle, it is useful to situate this thesis as focused primarily on the analysis section of the cycle.[125] Johnson's statement at the opening of this chapter that "[a]t the core of intelligence is the challenge of analysis" elevates the importance of analysis within the intelligence process.[126] Anthony Cordesman reinforces this perspective

---

[120] Michael Goodman, *Studying and Teaching About Intelligence: The Approach in the United Kingdom*, accessed on 4 March 2011 at: www.cia.gov/. Intelligence analysis as a field of research could be argued to have commenced in the United States during the late 1940s, reflected in the work of Sherman Kent at the CIA. Indeed, the CIA's establishment of the *Sherman Kent Centre for Intelligence Analysis* reflects Kent's influence on the intellectual development of the field. In the UK, Goodman argues that it was not until the mid-1970s that intelligence began to be pursued as an academic field. In Australia, the development of the intelligence analysis as an area of academic focus has been even more recent, and remains a fledgling field.

[121] These include: Sherman Kent, *Strategic Intelligence for American World Politics*, Princeton University Press, 1966; Richard Betts, Analysis, War and Decision: Why Intelligence Failures are Inevitable, *World Politics*, Princeton University Press, Vol.31, No.1, October 1978, pp.61-89; Walter Walter Laqueur, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, 1993; Michael Herman, *Intelligence power in peace and war*, Cambridge University Press, Cambridge, 1996; Richards Heuer, *The Psychology of Intelligence Analysis* Washington DC, Center for the Study of Intelligence, 1999.

[122] Michael Warner, Wanted: A Definition of "Intelligence", *Studies in* Intelligence, Vol.46, No. 3 Central Intelligence Agency, 2002, pp.15-22, p.15.

[123] Sherman Kent, Prospects for the National Intelligence Service, *Yale Review*, Vol.36, Autumn 1946, p.117 quoted in Michael Warner, Wanted: A Definition of "Intelligence", *Studies in* Intelligence, Vol.46, No. 3 Central Intelligence Agency, 2002, pp.15-22, p.18.

[124] For a description of the intelligence cycle refer to Director of Central Intelligence, *A Consumer's Guide to Intelligence*, Diane Publishing Company, March 1999, pp.viii-3.

[125] As a theoretical construct, the intelligence cycle is not without criticism. For a critique of the intelligence cycle see Arthur Hulnick, What's Wrong with the Intelligence Cycle, *Intelligence and National Security*, Vol.21, No.6, December 2006, pp.959-979.

[126] Loch Johnson, An Introduction to the Intelligence Studies Literature, ed. Loch Johnson in *Strategic Intelligence 1: Understanding the Hidden Side of Government*, Praeger Security International, Westport, 2007, p.5.

in his argument that improvements in collecting information are meaningless without improving analysis.[127] The issue, Mike McConnell argues, is that "[i]ntelligence can only help inform and shape decisions if it is processed through the mind of an analyst".[128] Indeed, the technologically-enabled collection of vast amounts of information is already being achieved by intelligence communities.[129] Thus, there appears much to be gained by focussing specifically on the analytical aspects of intelligence. Consequently, for the purposes of this thesis it is important to define the use of the terms *information*, *intelligence* and *intelligence analysis.*[130]

When speaking of intelligence as an end-product, it is widely accepted that there is a difference between *intelligence* and *information*, with intelligence regularly defined as information (often described as secret information[131]) with analysis and judgements applied.[132] For example, in addition to the process of acquisition, Richard Betts defines strategic intelligence as the "analysis and appreciation of relevant data".[133] In their 1976 book *Intelligence Research Methodology*, Jerome Clauser and Sandra Weir adopt a similar

[127] Anthony Cordesman, *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the US Homeland*, Centre for Strategic and International Studies, Washington, D.C., 2002, p.440.
[128] Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53.
[129] According to McConnell, the United States intelligence community collects over one billion pieces of information every day. Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53.
[130] Whilst the terms are defined for the purposes of the study, those quoted within these pages do not necessarily adopt these same definitions. Indeed, the interchangeable use of the terms intelligence and information is particularly apparent within the intelligence inquiries discussed in Chapters 5-7.
[131] For example, refer to: Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006, p.6; and Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors, House of Commons 898*, London, The Stationery Office, 2004, p.14.
[132] For a discussion of the numerous informational definitions of intelligence, refer to Michael Warner, Wanted: A Definition of "Intelligence", *Studies in* Intelligence, Vol.46, No. 3 Central Intelligence Agency, 2002, pp.15-22.
[133] Richard Betts, Analysis, War and Decision: Why Intelligence Failures are Inevitable, *World Politics*, Princeton University Press, Vol.31, No.1, October 1978, pp.61-89, p.61.

definition, arguing that "[i]ntelligence is evaluated information".[134] The strength, or at least longevity, of Clauser and Weir's definition is evident in its continued acceptance.[135] Thus, for the purposes of this thesis, information is defined as *data containing meaning* (data + meaning)[136], with intelligence as an end-product defined as *information which has been analysed* (information + analysis).[137] Defining intelligence as simply *analysed information* avoids unnecessarily narrowing the concept based simply on a notion of secrecy. Indeed, adopting a definition of intelligence as something 'special' based solely on 'secrecy' would appear to inculcate the field from valuable research within the information sciences, decision-sciences and cognitive psychology.[138] This thesis argues that information becomes intelligence once subject to analysis, regardless of the origin or classification of the information being assessed.[139] Whilst the issue of secrecy remains intimately linked with concepts of intelligence, such secrecy has actually served to inhibit the development of intelligence as a field of research.[140]

---

[134] Clauser, Jerome K., Weir, Sandra M., *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*, Washington DC, Defense Intelligence School, 1976, p.19

[135] For example, some 28 years later, Professor Ross Babbage provided a very similar definition of intelligence, arguing that that the difference between data or information and intelligence is that "[i]ntelligence is analysed and has judgment". Professor Ross Babbage quoted in Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.296.

[136] This definition comes of information comes from Luciano Floridi, *Is Semantic Information Meaningful Data?*, Philosophy and Phenomenological Research, Vol. LXX, No.2, March 2005, p.353.

[137] *Ibid.*, p.353.

[138] The emphasis on secrecy appears to focus on how information is collected (or the nature of information collected) rather than how information is analysed.

[139] This is particularly pertinent given the increasing focus al all source analysis, that is information which is both publicly available and classified.

[140] Given its classified nature, intelligence has traditionally been a difficult subject to research. Indeed, the problem of under-theorisation can be linked, in no small part, to the classified nature of the vast bulk of intelligence. However, in efforts to convince the public of threats or to meet public demands for inquiries into major attacks, governments have publicly released information, intelligence analysis and threat assessments made by intelligence agencies. These inquiries and government releases have provided an insight into analysis and threat assessments within years, even months, of major attacks. The public release of intelligence and intelligence-related material in a relatively timely manner now provides academic researchers with an opportunity to bring critical analysis to the field. This is not to suggest that important research has not been undertaken within the classified intelligence environment, however the lack of public access ultimately impacts on the intellectual credibility of such research as it lacks broad critical examination and is not subject to free and open intellectual debate. Additionally, the necessity of secrecy might also have

Similar to definitions of intelligence, there is no one agreed definition for intelligence analysis. Having defined intelligence as analysed information, it could be argued that intelligence analysis is a misnomer, and it could be described as *information analysis* and defined as *the analysis of information*. However, the term *intelligence analysis* is ingrained within the field and, to situate this study in the appropriate field of research, this thesis will use continue to use the term in this way. Defining intelligence analysis as *the analysis of information* is not to overlook (or attempt to oversimplify) what is an inherently complicated and complex endeavour involving both cognitive processes and analytic methods.[141] This complexity is apparent in Matthew Herbert's paper *The Intelligence Analyst as Epistemologist*. Herbert argues that "[i]ntelligence analysis is about coping with epistemic complexity. Its core imperative is to develop a clear estimate of the sum of knowledge derived from partial, multivariate information, and to balance that estimate against a postulate of what ought, in ideal circumstances, to be known in order to support a rational decision".[142] Similarly Richards Heuer, in his *The Psychology of Intelligence Analysis*, observes both the cognitive aspects of intelligence analysis whilst noting that understanding this process "…is hindered by the lack of conscious awareness of the

---

an unintended, negative impact on the critical examination of intelligence analysis. For example, Hayes describes the US intelligence community as "…a world in which the legitimate and often necessary resort to secrecy has served, all too often, to limit debate and discussion. It is a world in which the most fundamentally important questions—what if and why not—are too often seen as distractions and not as invitations to rethink basic premises and assumptions". Joseph Hayes, Afterword, in Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*, The Center for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2005, p.160. See also, Michael Goodman, *Studying and Teaching About Intelligence: The Approach in the United Kingdom*, accessed on 4 March 2011 at: www.cia.gov/

[141] In *Developing a Taxonomy of Intelligence Analysis Variables*, Johnson explores definitions of *intelligence analysis* across the literature, arguing that definitions tend to be based on either cognitive processes or analytical methods. Johnson adopts both cognitive processes and methodologies in his own definition of intelligence analysis: "…the socio-cognitive process by which a collection of methods is used to reduce a complex issue into a set of simpler issues within a secret domain". Johnson's definition also highlights the continued linkage of secrecy with definitions of intelligence analysis. For example see Rob Johnson, Developing a Taxonomy of Intelligence Analysis Variables: Foundations for Meta-Analysis, *Studies in Intelligence*, Vol.47, No.3, 2003.

[142] Matthew Herbert, *The Intelligence Analyst as Epistemologist*, International Journal Of Intelligence and Counterintelligence, Vol.19, 2006, pp.666-684, p.667.

workings of our own minds".[143] Heuer also goes some way in identifying the uncertainty facing analysts, noting that "[i]ntelligence seeks to illuminate the unknown. Almost by definition, intelligence analysis deals with highly ambiguous situations".[144] These observations emphasise a perception of intelligence analysis as a continual process of forming judgments and making decisions based on available information whilst dealing with inherent uncertainty.

A final point worth noting in any discussion of intelligence analysis is that intelligence analysis is not an end in itself. Instead, as Jack Davis observes, intelligence analysis exists to assist decision-makers in making sound decisions. In a statement also applicable within the context of the UK and Australia, Davis argues that "[t]he central task of intelligence analysis is to help US officials—policymakers, war fighters, negotiators, law enforcers—deal more effectively with substantive uncertainty, and especially to provide timely warning of military attacks and other threats to US national security interests".[145] Whether or not intelligence achieves such lofty aims, the growth of formal intelligence agencies, particularly in the 20th and 21st centuries, indicates that intelligence, at the very least, does assist officials in making decisions about threats. Indeed, the very existence of intelligence agencies indicates an assumption by governments that there is a degree of foreseeability in threats to the state.

Arguments over the under-theorisation of intelligence analysis are supported by the dominant use of one model for defining and describing threat. Indeed, the widespread

[143] Richards Heuer, *The Psychology of Intelligence Analysis*, Washington DC, Center for the Study of Intelligence, 1999, p.1.
[144] *Ibid.*, p.14.
[145] Jack Davis, *Improving CIA Analytic Performance: Analysts and the Policymaking Process*, Sherman Kent Center for Intelligence Analysis Occasional Papers: Vol.1, No.2.

acceptance of the conventional model of threat, without robust critiques or considerations of alternatives, hints at a lack of robust analytical debate within the field. Certainly, such a reliance on a single approach to assessing threat runs counter to the recurring expression for new concepts, new thinking and new approaches to the critical area of intelligence analysis.

Governments and intelligence agencies have themselves argued for new approaches and new thinking in intelligence analysis. The United States' *National Intelligence Strategy* argues for a need to "[s]trengthen analytic expertise, methods, and practices; tap expertise wherever it resides; and explore alternative analytic views".[146] Flood's investigation of Australian Intelligence agencies proposes that terrorism "…requires a range of new analytical approaches and methodologies".[147] Similarly, the Chairman of the UK's Joint Intelligence Committee, John Scarlett, made the recommendation that there is a requirement for "…new techniques and skills required to combat international terrorism".[148] The US Director of National Intelligence suggests that "US intelligence agencies will never have enough analysts to fully examine all the data they collect, but the ones they do have can do their job better by developing new ways of thinking about analysis and information distribution in a more integrated community".[149]

In the intelligence literature, there is a similar recognition of a requirement to improve

[146] Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005, p.5.
[147] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.36.
[148] John Scarlett (then Joint Intelligence Committee Chairman), *Annual Review by the JIC Chairman: 2003–2004*, quoted in Intelligence and Security Committee, *Annual Report 2004–2005*, The Stationery Office, 2005, p.19.
[149] Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53.

intelligence analysis. Indeed, in relation to non-state threats, such arguments for improving analytical aspects of the field of intelligence are prevalent. Arthur Hulnick writes that "[t]he intelligence community needs to develop a twenty-first century analytic culture that differs from the conventional intuitive analysis of the past".[150] Fredrick Hitz and Brian Weiss argue that "[u]npredictable threats and information overload require, now more than ever, creative analysts and new analytical techniques".[151] Bruce Berkowitz asserts that "…intelligence agencies must be fiercely proactive in collecting information on terrorists and must rustle the bushes to find a threat that is hiding. That requires different methodologies and a different operational mindset than prevailed during the Cold War".[152] Of particular note is Rob Johnston's effort at developing a taxonomy of intelligence analysis. Johnston's effort is aimed at developing intelligence analysis as a field of research in its own right, based on the argument that "[i]ntelligence needs methodologists to help strengthen the domain of analysis".[153] This is not to suggest that traditional methodologies are no longer relevant to analysis. As Alfred Rolington observes, while many of the Cold War intelligence techniques and processes remain valid, they by themselves will not be able to adapt to the changing threats of the twenty-first century.[154] Thus, the argument can be made that, given the changing nature and characteristics of threats, assumptions underlying existing approaches should be critically examined and new approaches considered. What is perhaps most surprising is that despite the expressed desire in government publications and the intelligence literature, the very model underpinning

[150] Arthur Hulnick, What's Wrong with the Intelligence Cycle, *Intelligence and National Security*, Vol.21, No.6, December 2006, pp.959-979, p.94.
[151] Frederick Hitz and Brian Weiss, Helping the CIA and FBI Connect the Dots in the War on Terror, *International Journal of Intelligence and Counter Intelligence*, Vol.17, 2004, pp.1-41, p.29.
[152] Bruce Berkowitz, The New Protracted Conflict: Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, Pages 289-300, p.292.
[153] Rob Johnston, Integrating Methodologists into Teams of Substantive Experts: Reducing Analytic Error, *Studies in Intelligence*, Vol. 47, No 1, 2003, pp.57-65, p.65.
[154] Alfred Rolington, Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.738-759, p.745.

threat has avoided detailed critique.

Chapter 2

The Ontology, Epistemology and Methodology of Assessing Threat: State versus Non-State

> Defining and describing "the threat" was easier during the forty years of cold war with the USSR, when estimators at the CIA hammered out the Annual Survey of Soviet Strategic Intentions and Capabilities.
>
> Thomas Powers[1]

2.1 Ontology of Threat

Ontology:
The study of existence, and the nature and characteristics of entities. In this thesis, the ontological problem is the nature and characteristics of entities that threaten and are threatened.

A discussion of the ontology of threat, including defining threatening and threatened entities, is critical prior to critiquing the epistemology and current methodology of threat assessment. This section examines the nature and characteristics of threatening entities and defining what, or who, it is that they threaten. As Eric Little and Galina Rogova argue, "[t]hreat is a very complex ontological item and, therefore, a proper threat ontology must be constructed in accordance with formal metaphysical principles that can speak to the complexities of the objects, object attributes, processes, events and relations that make up

[1] Thomas Powers, *Intelligence Wars: American Secret History from Hitler to al-Qaeda*, New York Review Books, New York, 2004, pp.396-397.

these states of affairs".[2] An ontology of threat is therefore fundamental to a critique of the conventional model of threat.

Threats do not exist in a vacuum. Björn Müller-Wille's argument on security and threats helps to illuminate the interrelationship between threatening and threatened entities. According to Müller-Wille, "[l]ogic prescribes that anyone who speaks of security has to refer to something that can be threatened. If a threat is not a threat to something, it is not a threat. When speaking of threats and security these two words must always refer to something that is threatened or secure".[3] Thus, for a threat to exist, it must be in reference to something. For intelligence analysis, this requires that analysts define both what a threat is, and what is being threatened. Despite this critical inter-relationship between threatening and threatened, it is threatening actors that tend to dominate intelligence analysis, with definitions of who or what is threatened often assumed rather than explicitly defined.[4] Nonetheless, without an understanding of who or what is being threatened, attempts at assessing threat are potentially meaningless. Thus, a meaningful ontology of threat must include both threat and threatened entities.

Developing an ontology of threat requires a taxonomy. A potentially useful taxonomy used in describing *security* analysis is provided by Buzan, Waever and Wilde.[5] They argue that

---

[2] Eric Little and Galina Rogova, An Ontological Analysis of Threat and Vulnerability, in *Proceedings of the FUSION 2006-9th International Conference on Multisource Information Fusion*, July 10–13, Florence, Italy, 2006.

[3] Björn Müller-Wille, *Thinking security in Europe - Is there a European Security and Defence Identity?*, Münster, 2003, (PhD Thesis), p.16, available at: http://miami.uni-muenster.de/servlets/DerivateServlet/Derivate-1501/dissertation.pdf

[4] A similar argument is evident in Flynn *et. al.* in their recent review of US intelligence efforts in Afghanistan. Michael Flynn, Matthew Pottinger, and Paul Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Centre for a New American Security, Washington, D.C., January 2010, p.21.

[5] Barry Buzan, Ole Wæver, Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder, 1998. The idea of adapting Buzan, Wæver and Wilde's concept of security entities to

security analysis involves three distinct actors:

- a *referent object*, who is threatened and needs protecting;
- a *securitizing actor*, who undertakes a *securitization move*, i.e. decides upon what is threatened and what is threatening; and
- *functional actors*, who are neither the referent object nor securitizing actor but influence the dynamics of one of five political sectors (military, environmental, economic, societal, political).[6]

This taxonomy can be adapted for intelligence analysis to describe the entities which make up threat. For the purposes of this thesis, the entities defined in a taxonomy of threat are:

- a *referent* is what, or who, is threatened;
- an *analyst* acts as a *'determiner of threat'* (equivalent to *securitizing actor*); and
- a *threat actor* who is assessed by the *analyst* as threatening the *referent*.[7]

Having defined these three basis entities, we can commence with an analysis of these three entities of threat.

---

develop an ontology of threat was influenced by Björn Müller-Wille's adaptation of Buzan et al. in his considering of a concept of a European Security and Defence Identity (ESDI). See Björn Müller-Wille, *Thinking security in Europe - Is there a European Security and Defence Identity?*, Münster, 2003, (PhD Thesis), pp.16-17, available at:
http://miami.uni-muenster.de/servlets/DerivateServlet/Derivate-1501/dissertation.pdf. Müller-Wille

[6] Barry Buzan, Ole Wæver, Jaap de Wilde, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder, 1998, p.36.

[7] The nearest equivalent to the *threat actor* that Buzan et al. employ is the concept of *functional actors*. This, however, does not fully capture the idea of a *threat actor*. If one adopted Buzan et al's model for *security* analysis, an argument could be made that a *threat actor* presents as a sub-unit from within the broader unit of *functional* actors.

The traditional focus of security and defence has been about protecting the state from attacks by other states.[8] Within this context, the *referent* of threat was the state, specifically the survival of the state and its population.[9] Whilst state-survival remains the ultimate priority of security and defence, priorities also include the protection of state interests and individual citizens both within and beyond the borders of the state.[10] This is evident in Australian, UK and US government publications:

- Australia's *National Security Strategy* highlights the Government's responsibility for "[p]rotecting Australians and Australian interests both at home and abroad".[11]
- *The National Security Strategy of the United Kingdom* argues that "[p]roviding security for its citizens remains the most important responsibility of government…", whilst highlighting that "…our view of national security has broadened to include threats to individual citizens and our way of life, as well as to the integrity and interests of the state".[12]
- The *Quadrennial Homeland Security Review* outlines security as the requirement to "[p]rotect the United States and its people, vital interests, and way of life".[13]

The globalisation of state interests, due to increasing interconnectedness between states

[8] Sir David Ormand, *The National Security Strategy: Implications for the UK intelligence community*, Institute for Public Policy Research, Discussion Paper, February 2009, p.4.
[9] Within Singer's paper, the referent could be defined as survival of the United States. This is evident in his description of decision-makers as conscious of their responsibility "…for the protection of the nation from outside enemies". J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.
[10] Sir David Ormand, *The National Security Strategy: Implications for the UK intelligence community*, Institute for Public Policy Research, Discussion Paper, February 2009, p.4.
[11] Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008.
[12] Cabinet Office, *The National Strategy of the United Kingdom: Security in an interdependent world*, The Stationery Office, London, March 2008, pp.3-4.
[13] Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, Washington, D.C., February 2010, p.ix.

and non-state actors, and the movement of citizenry globally, makes clear identification of a state's interests, even population distribution, increasingly difficult.

A state is well-established, well-accepted geo-political concept, defined in international law. States largely have a well-defined geography, population, history, and clearly identifiable political and military hierarchies. This is not to suggest that all states are cohesive, coherent or effective. The recent history of Somalia provides one example of a state without a functional central government or bureaucracy administering the state.[14] Nevertheless, states remain the principal internationally-accepted geopolitical entity. Under the *Montevedio Convention*, the four broadly accepted requirements for statehood are: a permanent population; defined territory; a government; and the ability to enter into relations with other states.[15] These requirements broadly relate to four aspects of a state that can be threatened, namely:

- Population
- Territory
- Government
- Interests

Having identified these four factors of states which can be threatened, attention turns to the nature and characteristics of state-based and non-state threats and considers how these

[14] For an extended discussion on the anarchic condition of many states, refer to Robert Kaplan's 1994 article, *The Coming Anarchy*. Kaplan makes the argument that for many parts of the globe, poor governance and ineffective security means that the geo-political map does not reflect the chaotic nature of these areas. Robert Kaplan, *The Coming Anarchy*, The Atlantic Monthly, February 1994, at: http://www.theatlantic.com/doc/199402/anarchy accessed 29 June 2009.
[15] Montevideo Convention, 26 December 1933, accessed at: http://avalon.law.yale.edu/20th_century/intam03.asp on 07 May 2010.

entities can threaten these four factors.

Given the size and resources available to states, potential threats from other states remain a principal concern for governments. The definition of the state provided above illustrates that state-based threats can be identified relatively easily. Therefore, while the there can be vast differences between states (i.e. population, geography, governments and economies), the concept of a state provides a framework which enables the state-based threats can be understood, compared and contrasted. As Gregory Treverton argues, intelligence analysts and policy officials know what states are like, even states different to their own. Consequently, they have a 'shared story' about states.[16] States are largely delineated from other states, having known borders and capitals, and mostly behaving in a manner that is openly observable.[17] So what are the threats presented by states to other states?

A primary and enduring concern for states has been deterring enemies and defending the state's territory against external aggression from other states.[18] Despite an increased attention to non-state threats, government publications demonstrate that concern over conventional warfare between states remains central to concepts of security of the state. The United Kingdom's 2009 *National Security Strategy* highlights that concepts of security during the twentieth century was dominated by threats from states.[19] Whilst arguing that the UK does not currently face a military threat from another state (based upon assessments of states' intentions and capabilities), it is telling that the first type of

[16] Gregory Treverton, *Next Steps in Reshaping Intelligence*, RAND, Santa Monica, 2005, p.18
[17] Warren Fishbein and Gregory Treverton, *Making Sense of Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004.
[18] For example, the *Strategic Basis of Australian Defence Policy*, March 1971, para 78, examined the threat of Indonesia mounting a "…serious and sustained attack on the Australian mainland".
[19] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, pp.10 & 19.

threat to be assessed in the *Strategy* are state-based.[20] As noted by the United Kingdom's, *Development Concepts and Doctrine Centre,* the defence force remains the "ultimate insurance policy" against state-based threats.[21] The focus on deterring and (potentially) defeating state-based threats is similarly prominent in Australian and United States Defence White Papers. The 2009 Australian Defence White Paper is cognizant of Australian geography and the maintenance of territorial integrity, arguing the need for "…contingency plans for the defence of Australia and its approaches…" that need to address "…sea control and air superiority in our approaches, the defence of our offshore territories and resources, and operations on and around our territory".[22] This is based on the premise that the defence of Australia against armed attack remains the core strategic interest for Defence. The US Quadrennial Defense Review remains focused on state-based threats, whilst noting the US's dominance in large-scale force-on-force warfare. The argument is that the US has a continued requirement to be prepared to defeat "…aggression by adversary states, including states armed with…nuclear weapons".[23] Recent conflicts with insurgencies in Iraq and Afghanistan, and the continued efforts to adapt to counter-insurgency (COIN) operations, have highlighted that the many state militaries have previously been structured for countering state-based threats.

Related to the threat to territory is the threat to citizenry, namely protection of the population from conventional warfare between states. In terms of potential killing power, the greatest threat to states' populations remains the WMD capabilities held by states. Even

[20] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, p.10.
[21] Ministry of Defence, Future Character of Conflict, *Development Concepts and Doctrine Centre*, Shrivenham, 2010, p.2.
[22] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p.51.
[23] Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 2010, p.15.

without WMD, conventional warfare between states can still threaten the lives of millions of citizens due to the killing power and resources available to many states. Whilst the lessening of hostilities between major powers has occurred since the end of the Cold War, the potential harm that state-based conflict can have on entire populations remains. Short of conventional warfare, state-sponsored mass-casualty attacks are also an avenue for state-based threats against citizens.[24]

The threat to a government and its ability to exercise power can also be threatened by other states, particularly within the context of conventional warfare, sanctions, blockades or intimidation. Many state governments' ability to exercise political power over their territory and population is more readily threatened by internal conflicts. However, within developed states, threats to political sovereignty are more likely to come from other states. Thus, the "maintenance of political sovereignty" against external state-based threats remains a priority of governments.[25]

State interests often lack deliberate definitions, although there are several commonly identified interests which can be threatened by other states. These include threatening a state's political influence, thus limiting the state's ability to develop favourable or strong relationships with other states. State-based threats to regional stability and a rules-based international system are regularly highlighted as a potential impact on state interests.[26] A state's economic stability, development and financial infrastructure are consistently

[24] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, p.10.
[25] Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008.
[26] For example, refer to Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p. 43; and the Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 2010, p.9 which argues that "America's interests are inextricably linked to the integrity and resilience of the international system".

identified within government publications as interests that can be threatened by other states.[27] Often related to economic interests is the ability to threaten another state's opportunity to trade, including access to markets, energy resources, lines of communication and the ability of citizenry to travel.[28]

In many cases, the most serious state-based threats remain *potential* rather than actual. This is currently the situation in developed states, which are not currently engaged in conventional wars against each other states. Conflicts between states have continued in this century, most notably between a US-led Coalition force in the war on Afghanistan (2001) and the US-led Coalition force in the war on Iraq (2003). Both of these Coalitions included the United Kingdom and Australia. Of note, what could be described as the conventional combat phases between opposing states lasted a matter of months in each case. In contrast, the lengthy and currently ongoing conflicts in Afghanistan and Iraq have been between US-led Coalition forces (state-based militaries) and insurgencies (non-state actors). However, conflicts between states remain limited. As a result, state-based threats to territory, population, and governments are more likely to be potential than actual. Actual state-based threats are more likely to be to other states' interests which, it could be argued, are a constant (albeit largely bloodless) state of conflict. Non-state threats, on the other hand, represent both a potential and an *actual* threat. One might argue that this could be seen as delineating between peace and war in threats from states, whereas non-state actors may potentially see themselves as in a constant state of war.[29]

---

[27] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, p.10.
[28] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p.42.
[29] Osama bin Ladin's 1996 and 1998 *fatwas* declaring *jihad* against the United States provide an examples of this. My thanks to an anonymous reviewer for this observation.

Unlike states, non-state actors do not necessarily present as bounded or well-understood threat actors. Whereas states are well-defined, non-state actors (particularly threatening ones) are often ill-defined. An immediate limitation in defining non-state threats is the term non-state actors. Non-state actors are defined by what they are not (i.e. not a state) rather than by what they are. Consequently, almost any entity meets the definition of non-state actor. A useful definition for capturing the scope of entities that can be defined as non-state actors is "…any person or group of people who act independently of formal governments".[30] Given that all entities (apart from states) meet this definition it is apparent that not all non-state actors are threats. The breadth of actors included within this definition underscores the difficulty in reaching even the most generic conclusions about the nature and characteristics of non-state actors. Treverton argues that, unlike the shared stories of states, "[t]here is much less of a shared story about non-states, which come in many sizes and shapes. Their forms combine network and hierarchy. Understanding them is less bounded, and more outcomes are possible".[31] While states are geographically bound, with most changes occurring within well-defined physical borders, non-state actors can exist both within and across state boundaries, adding a significant level of complexity to any attempt to understand their nature and characteristics. This is not to suggest that states are not complex. Instead, the point is that states represent a familiar actor within a well-established context in contrast with what is potentially an unfamiliar and potentially ill-defined non-state actor. Unlike the overt nature of states, non-state actors (at least those that threaten states) may attempt to conceal their very existence. Even when the existence of non-state actors is known, these entities often are inherently difficult to understand or accurately assess.

[30] Department of Defence, *Future Warfighting Concept*, Commonwealth of Australia, Canberra, 2002, p.8.
[31] Gregory Treverton, *Next Steps in Reshaping Intelligence*, RAND Corporation, Santa Monica, 2005, p.18.

Bruce Hoffman's caution in 2003 against declaring any defeat of Al Qa'ida in the light of continued disagreement "over precisely what Al Qaeda is" underscores the critical importance of understanding the nature of non-state threats.[32] Brian Jackson supports this argument, noting that:

> Counterterrorism officials and policymakers at all levels frequently use the term Al Qaeda [*sic*] differently—to refer to the source of detected or suspected terrorist activity that may be connected to Osama bin Laden, to individuals with direct contact to him, to affiliate groups supported through his access to funds or charities, or to individuals inspired by his public statements and ideologies.[33]

According to Jackson, these definitional and linguistic problems reflect a change in the nature of non-state threats from "…comparatively well-defined, contained, and stable organizations—such as "classic" left-wing groups in Europe where the small size and tight organization meant choosing a single label for the group and all its activities did not pose any difficulty—to acts taken by broadly spread out, amorphous organizations that, while held together by a common ideology, may lack any strong or direct linkages among members".[34] Certainly definitions and distinctions matter, and yet it is apparent that efforts at defining specific non-state actors can be a problematic endeavour. The description of non-state actors, like Al Qa'ida, as "a networks of networks of networks"[35] gives an

---

[32] Bruce Hoffman, Al Qaeda, Trends in Terrorism, and the Future Potentialities: An Assessment, *Studies in Conflict and Terrorism*, Vol.26, 2003, pp.429-442, p.431.

[33] Jackson argues that the selection of terms used to describe and define the boundaries of groups is critical as these terms influence how policymakers perceive the threat and the counterterrorism efforts selected. Jackson presents an argument for using command-and-control structures within an organisation as a method for defining the organisation using one of three categories: a network; a network; or a movement. Brian Jackson, Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda, *Studies in Conflict & Terrorism*, Vol.29, 2006, pp.241–262, p.242.

[34] *Ibid.*, p.242.

[35] Frank Cilluffo, Ronald Marks, and George Salmoiraghi, The Use and Limits of US Intelligence, in Loch Johnson and James Wirtz (Eds.), *Strategic Intelligence: Windows Into a Secret World*, Roxby Publishing Company, Los Angeles, 2004, p.35.

indication of the difficulty in attempting to determine the boundaries of non-state threats, except at the most abstract level. Indeed, even after years of analysis of Al Qa'ida, experts still disagree over the group and the threat that it presents. Bruce Hoffman and Marc Sageman's debate over Al Qaeda's leadership and the concept of "Leaderless Jihad" is an example of the disagreements between experts over the nature and threat from even well-known, though not necessarily well-understood, non-state actors.[36]

Non-state actors do not necessarily present themselves on the same scale as states and the potential threats they pose, and this is due, quite simply, to the scale of resources that states can draw upon.[37] In addition, the types of threats presented by a non-state actor can also be *potentially* posed by state-based threats. Again, in identifying what non-state actors can threaten, this section will consider threats to a state's territory, population, government and interests. In the context of civil wars, insurgencies and revolutions, non-state actors can threaten the territory and sovereignty of a state. Indeed, since the end of World War Two, it is wars within states rather than wars between states that represent the most common and deadliest conflicts globally.[38] The principal concern over non-state threats in the US, UK and Australia is not necessarily threats to these states' territory. Similarly, non-state actors (either external or internal to these states' geography) do not currently appear to present a threat to these states' governments or their political sovereignty.[39] Instead, the primary focus is on non-state threats to the population and state interests.

---

[36] See Marc Sageman and Bruce Hoffman, Does Osama Still Call the Shots?: Debating the Containment of al Qaeda's Leadership, *Foreign Affairs*, Vol.87, No.4, July/August 2008, pp.163-167.

[37] In saying this, more people were killed in the 11 September 2001 attacks by Al Qa'ida killed more people than in the Japanese bombing of Pearl Harbour in 1941.

[38] Refer to: Milton Leitenberg, *Deaths in Wars and Conflicts in the 20th Century*, 3rd Edition, Cornell University Peace Studies Program, Occasional Paper No.29, 2006 at: http://www.clingendael.nl/publications/2006/20060800_cdsp_occ_leitenberg.pdf.

[39] One possible exception was the potential attempt by a non-state actor to influence the outcome of the Spanish general election with the 11 March 2004 Madrid bombings. The extent to which the government's policies and reaction to the bombings resulted in its electoral defeat, held on 14 March, remains a matter for debate.

Potential and actual non-state threats to citizenry are consistently highlighted in government publications, along with the requirement to protect citizens from mass-casualty attacks both within the state and whilst overseas.[40] Non-state actors do not generally threaten a state's entire population, as the threat of nuclear warfare between states might. However, the fact that mass-casualty attacks have actually been carried out has sharpened governments' attention to this non-state threat.[41] In addition, concern about non-state actors' potential acquisition and use of WMD continues to be assessed as a viable threat to cause mass-casualty events.[42] The priority governments give to protecting citizens highlights the context within which governments of developed states currently perceive the principal threat from non-state actors.

Non-state threats to state interests are consistently highlighted within government publications. The importance of a stable, rules-based international system is regularly identified as in states' interests.[43] It can be argued that the use of force by non-state actors threatens a basic tenant of the international rules-based system which is that only states can legally employ force. Thus, through specific attacks and the ongoing threat of violence, non-state actors can threaten regional and international stability. The non-state threat to

[40] For example, refer to: United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.14; National Security Council, *National Strategy for Combating Terrorism*, Washington, D.C., September 2006, p.24; and Department of Foreign Affairs and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004, p.xii.
[41] Counter-terrorism strategies and plans since 2001 within the United States, United Kingdom and Australia have regularly been published shortly after successful mass-casualty attacks.
[42] United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.9; National Security Council, *National Strategy for Combating Terrorism*, Washington, D.C., September 2006, p.14; Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland* , Washington, D.C., February 2010, pp.6 and 40.
[43] Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009, p.43; Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 2010, p.9; Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an interdependent world*, The Stationery Office, London, 2008, p.6.

states' economies and economic interests is an ongoing concern, particularly given that most states are linked into the global economy.[44] The World Bank estimated that the 11 September 2001 attacks reduced global GDP by almost 1%.[45] Specific attacks can also threaten a state economically in costs to economic productivity, loss of critical infrastructure and reconstruction costs. Economic costs can also include state actions aimed at preventing further attacks.

To sum up, to-date the scale of non-state threats to developed states is considered to be lower than the *potential* scale of state-based threats. Current concerns about non-state threats focus principally on their threat to states' populations and interests rather than territory or political sovereignty. Nevertheless, it is both the actual and potential threats from non-state actors that have promoted the relative importance that governments have given to identifying and addressing these threats.

The third actor defined in the ontology of threat is the *analyst*. The analyst is the individual who assesses both the threat actor and referent. Whilst the analyst is acknowledged as a part of the ontology of threat, the primary concern of this thesis is on threat actors and, to a lesser degree, referent objects. In terms of analysis, this thesis is interested in the epistemology and methodology used by analysts, rather than the analyst's cognitive processes.[46] A summary of threat actors and referents within the context of the US,

[44] Department of Foreign Affairs and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004, p.xii.
[45] Cabinet Office, *The National Security Strategy of the United Kingdom: Security in an interdependent world*, The Stationery Office, London, 2008, p.7.
[46] A critical focus on the analyst requires research into cognitive aspects of individual analysts, and of analysts as a group, requiring research into fields of psychology, ethnography and anthropology. Research into the individual and group psychology of analysts is beyond the scope of this thesis, though there has been important research into the analyst and intelligence agencies in the field. Some notable examples include Richards Heuer's *The Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Central

Australia and the UK, as discussed above, is displayed in the following table.

		Threat Actor	
		States	Non-state actor
		195 potential threat actors[47]	6.9 billion potential threat actors[48]
Referent	Population	- Conventional warfare - Mass-casualty attacks	- Mass-casualty attacks
	Territory	- Conventional warfare	- No
	Government	- External threats to Government	- No
	Interests	- Political influence - Regional stability - Rules-based international system - Economy - Infrastructure - Trade - Access	- Regional stability - Rules-based international system - Economy - Infrastructure - Trade - Access

Table 1: Ontology of Threat: Threat Actors and Referents

Intelligence Agency, Washington, D.C., 1999; Rob Johnson, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2005; and Jeffrey Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., December 2005.

[47] Based upon United Nations member states as well as Kosovo, Taiwan and the Vatican City.

[48] Number based upon estimates on http://www.census.gov/ipc/www/idb/ as at 03 March 2011.

2.2 Epistemology of Threat Assessment

Epistemology:
Study of the nature of knowledge in a particular field. In this thesis, it is the study of the knowledge of threat and how threat is understood within the field of intelligence analysis.

As demonstrated in Chapter 1, the concept of threat described by Singer has been a foundational concept in intelligence. Consequently, the parameters of *intent* and *capability* can be described as the dominant episteme used to understanding threat within the field of intelligence analysis. As noted, this thesis avoids a debate over semantics, noting that similar terms can be used in place of *capability* and *intent*, such as *means* and *will*. However, it is argued that these terms are not fundamentally different and, therefore, are simply semantic changes to what remains an actor-based approach. The argument is that replacing the current parameters with similar parameters would not address the assumptions underpinning, or limitations of, the approach. Having defined the three actors within an ontology of threat, it is apparent that the conventional model of threat deals only with one: the threat actor. It is the threat actor's intentions and capabilities which form the basis for Singer's approach to understanding threat.

An ongoing debate within the intelligence literature has been over which of the two parameters analysts should focus their attention on. However, rather than a genuine critique of the dominant episteme this is more appropriately described as a debate *within* the framework. That is, alternating between parameters, depending upon the problem at hand, can be seen more as an attempt to validate the approach rather than identify

limitations of the approach. As is highlighted in the next paragraphs, the literature provides an insight into the lack of critique of Singer's model and highlights how the debate has failed to progress, irrespective of whether the focus is on state-based or non-state threats.

Perhaps the first to take up this debate in a public forum was Samuel Huntington, in *The Soldier and the State* (1957), in which he argues that military personnel are qualified to assess *capabilities,* but not *intentions*.[49] In the early 1960s, Glenn Snyder, in *Deterrence and Defence: Toward a Theory of National Security*, observed that the threat of nuclear weapons had emphasised the importance of understanding intentions over capabilities.[50] Capabilities were assumed to be a given. According to Mark Lowenthal, the mid-1970s witnessed a "capabilities versus intentions debate" within US intelligence and policy communities, as the perception was that US intelligence was thought to understand Soviet capabilities fairly well, but not Soviet intentions.[51] Most notable during this debate was Raymond Gartoff's paper *On Estimating and Imputing Intentions*. Gartoff described the argument to "only estimate capabilities" as a fallacy which had resulted a tendency to overestimate the USSR's potential for military development, assumptions that the USSR would maximise military capabilities, and that military development was usually assumed to indicate hostile intentions.[52] Consequently, this approach would see intentions as a dependent variable rather than as an independent parameter of threat.[53] Nevertheless, whilst critiquing the argument of estimating only capabilities, Gartoff's argument on fallacies of intent estimation remains part of the debate within the frame of Singer's model.

---

[49] Samuel Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations*, Vintage Books, New York, 1957, pp.66-67.
[50] Glenn Snyder, *Deterrence and Defense: Toward A Theory of National Security*, Princeton University Press, Princeton, 1961, p.49.
[51] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006.
[52] Raymond Gartoff, *On Estimating and Imputing Intentions*, International Security, Vol.2, No.3, Winter 1978, pp.22-32, p.24.
[53] My thanks to an anonymous reviewer for this suggestion.

The debate between the parameters is an ongoing one. Even with increased attention and priority given to identifying non-state threats, the capabilities-versus-intentions debate continues. For example, Cordesman argues that analysing threats "…from foreign terrorists and extremists require a focus on current and future capabilities, rather than on current intentions".[54] By contrast, John Sullivan argues that whereas assessments of Soviet capabilities were critical to understanding threat during the Cold War, the more important focus today is the need to understand "*Jihadi* intentions".[55] Based on a recent re-examination of the 1983 Beirut Marine Barracks bombings, Erik Dahl argues that "…the relationship between capabilities and intentions is reversed…" in that analysts "…while certainly still looking for indications of terrorist intentions, have found that determining enemy capabilities – what kind of weapons do they have, and where can they operate? – is at least as challenging and important".[56]

The perception that threat assessment is based on estimates of capabilities over intentions when dealing with non-state threats is reflected in observations by intelligence officials. For example, in testimony the Director of National Intelligence, Mike McConnell, argued that "…the big change for me, as an intelligence analyst in the community – back in the Cold War it was very easy to do capability and always difficult to determine intent. In this situation [post-Cold War terrorism threat], it's very difficult to capture the capability – a single human being in a given place, nuclear material, or whatever, so capability is the

[54] Anthony Cordesman, *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the US Homeland*, Centre for Strategic and International Studies, Washington, D.C., 2002, p.51.
[55] John Sullivan, The Frontiers of Global Security Intelligence: Analytical Tradecraft and Education as Drivers for Intelligence Reform, *Small Wars Journal*, accessed at: http://smallwarsjournal.com/blog/journal/docs-temp/87-sullivan.pdf on 3 March 2011.
[56] Erik Dahl, Warning of Terror: Explaining the Failure of Intelligence Against Terrorism, *The Journal of Strategic Studies*, Vol.28, No. 1, 31 – 55, February 2005, p.49-50.

challenge but intent is clear".[57] By contrast, in *Curing Analytic Pathologies*, Jeffrey Cooper argues that the threat presented by smaller and more agile adversaries involves "…more focus on their intentions and plans and less on large physical objects and weapons systems".[58] Cooper's observation is particularly interesting as it illustrates that even when researchers are specifically discussing the issue of analysis and alternative approaches, this debate *between* the parameters remains. Nevertheless, such a debate does not, it is argued, present a *critique* of the dominant episteme of threat, but rather simply represents an argument over *which* of the parameters of Singer's model to focus attention on. What these debates do illustrate, however, is the continued dominance of the traditional model for assessing and conceptualizing threats. Despite the shift to include assessments of non-state actors as a priority, threat remains defined using just one model, and that model is focussed singularly on the threat actor.

The adoption of this episteme contains within it the assumption that analysts *already* know and understand the threat actor they seek to assess. Without knowledge of an actor, there cannot be an assessment of either intent or capability. Consequently, this approach can be described as an *actor-based approach* to threat assessment. That is, the assessment of threat is reliant upon a knowledge and understanding of an actor.[59] An insight into the fundamentals of an actor-based approach is captured by Christopher Daase and Oliver Kessler in their description of the political construction of *danger*. Daase and Kessler list three criteria that need to be met for a threat to actor A to exist:

---

[57] Mike McConnell, Director of National Intelligence (DNI), testimony to the Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007.

[58] Jeffrey Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, Centre for the Study of Intelligence, December 2005, Washington, D.C., p.24.

[59] My acknowledgement to Lieutenant Colonel (Dr) David Kilcullen for his assistance in articulating this argument and his insights into actor-based and environment-based methodologies in the assessment of threat.

1. There is another actor, B, that can be identified as such;
2. An intention of actor B needs to be recognizable and pose a risk of harm to actor A; and
3. There is a potential instrument available by which actor B can inflict some considerable damage on actor A.[60]

These three criteria provide a sound basis for understanding the basic elements of an actor-based approach to assessing threat. It is evident that Singer adheres to these criteria in describing how the model is used to make decisions on whether or not a state represents a threat. The actors are well-known and clearly defined states: the Union of Soviet Socialist Republics; the United Kingdom; and Egypt.[61] Against each of these state actors, Singer considers whether US decision-makers and intelligence analysts would view them as threatening based on assessments of both a *recognisable intention* (based on the political hierarchy) and a *potential instrument available to harm* the US (nuclear weapons). Consequently, there is no consideration given to the problem of identifying threat actors using an actor-based approach. Identification is assumed. Some forty years later, Richard Betts employed an almost identical application of this approach, when arguing that:

> A threat consists of capabilities multiplied by intentions; if either one is zero, the threat is zero. For example, both Britain and France have the capability (in their SLBM warheads) to incinerate several dozen American cities, but US warning officers spend no time at all worrying about this because they know that there is no intention in London or Paris to do this. They face the reverse situation with Libya or Iran, where there is ample reason to worry that either one might well attempt to

[60] Christopher Daase & Oliver Kessler, Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger, *Security Dialogue*, Vol. 38, No. 4, 2007, pp. 411-434, pp.422-423.
[61] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.

> launch a nuclear attack on the United States if it could, but no reason *yet* to worry that they can.[62]

Where the focus is on state-based threats, identification of threat actors is a given as states are overt entities. Thus, debate during the Cold War did not focus on whether or not the USSR existed, but over the threat that it posed to Western nations. More broadly, at the time Singer was published, all *potential* threat actors with nuclear weapons were known to exist.[63] However, when addressing non-state threats, the assumption that all threats are already known to exist, or are clearly identifiable, is not a given. Indeed, as discussed below, it is arguably only United Kingdom's intelligence officials who have, at least publicly, acknowledged the sheer scale of the analytical problem.

Discussing the threat of terrorism within the United Kingdom, the then Director of the United Kingdom's Secret Service, Eliza Manningham-Buller, observed that the first analytical challenge in assessing non-state threats is identification. Manningham-Buller argued that "[t]he first challenge is to find those who would cause us harm, among the 60 million or so people who live here and the hundreds of thousands who visit each year".[64] According to Manningham-Buller, at the time of her speech in 2006, MI5 and police were addressing the threat of around 200 identified groups or networks, made up of over 1600 identified individuals within the UK and overseas who were involved in planning or facilitating terrorist acts.[65] Just one year after Manningham-Buller's speech, the new

---

[62] Richard Betts, Intelligence Warning: Old Problems, New Agendas, *Parameters*, Spring 1998, pp.26-35. SLBM stands for submarine-launched ballistic missiles.
[63] At the time Singer was writing (1958), only three states possessed nuclear weaponry: the United States, the USSR and Great Britain. Additionally, each of these states were known to have developed these weapons. Indeed, as a form of deterrence, it was in these states' interests to ensure it was known that they were armed with nuclear weapons in order to deter other states from attacking them.
[64] Eliza Manningham-Buller, *Terrorist Threat to the UK: MI5 Chief's full speech*, 9 November 2006, Times Online, published 10 November 2006.
[65] *Ibid*.

Director-General of MI5, Jonathan Evans, revealed a 25% increase in the number of individuals that the agency was aware of in relation to terrorism.[66] Additionally, Evans argued that MI5 believed that there were a similar number of threatening individuals that the agency remained unaware of. In 2009, the United Kingdom's Intelligence and Security Committee (ISC) observed that "[w]e would suggest that there are a great deal more people out there who pose a threat to the UK, beyond those known to MI5".[67] The issue of identification presents as an immediate problem in assessing non-state threats; something that was not necessarily considered in an actor-based model previously applied largely to state-based threats.

The conclusion here is a subtle, and yet critical, one: the actor-based approach described by Singer was not designed for *identifying* covert non-state threats, but for *assessing* overt state-based threats. An actor-based approach assumes knowledge and understanding of the actor being assessed. Whilst there are no unknown states, there are unknown non-state actors. Therefore, with non-state threats, the assumption of prior knowledge and understanding does not necessarily hold. Indeed, if the existence, nature or characteristics of non-state actors are unable to be accurately identified or understood, any assessment of that group's *intentions* and *capabilities* will be partial, and perhaps even potentially misleading or entirely incorrect.

As has been demonstrated, the dominant episteme of threat is based on an understanding of

[66] According to Evans, the increase was based on a number of factors including both an increased coverage of networks as well as new recruits. Jonathan Evans, *MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust*, 5 November 2007, accessed at: www.cfr.org/publication/14789/mi5_director_generals_speech_on_intelligence_counterterrorism_and_trust_html on 9 May 2009.

[67] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2009, p.55.

a threat actor's intent and capability. Consequently, threat assessment immediately defaults to the threat actor, with the referent often assumed or overlooked. Yet, as previously highlighted, a threat only exists in reference to something (or someone). This requirement to focus attention on the referent of threat, whilst not necessarily having surfaced as an assumption, is evident in extensions to the dominant episteme.

Several researchers have made adaptations to Singer's model through the addition of parameters.[68] These extensions to the model appear to capture the idea that understanding threat is not simply about the assessing a threatening actor. The most common parameters added to the dominant episteme are *vulnerability* and *opportunity*. At times these parameters have been expressed in quasi-mathematical form, mirroring Singer's original concept. [69]

The parameter of *vulnerability* is a factor focussed on the referent of the threat, rather than on the threat actor, which is the traditional focus of Singer's model. Consequently, vulnerability can be defined as *susceptibility of a referent to an attack*. To take one example of its use as an addition to the dominant episteme, Richard Pilch employs the following quasi-mathematical formula *Threat = Vulnerability x Capability x Intent* to

[68] For example, refer to: Eric Little and Galina Rogova, An Ontological Analysis of Threat and Vulnerability, in *9th International Conference on Information Fusion*, 10-13 July 2006; Richard Pilch, The Bioterrorist Threat in the United States, in Russell Howard and Reid Sawyer (Eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004; Alan Steinberg, Threat Assessment Technology Development, in Anind Dey, Boicho Kokinoc, David Leake, Roy Turder (Eds.), *Modeling and Using Context*, 5th International and Interdisciplinary Conference: Context 2005 Proceedings, Springer, Berlin, 2005, pp.490-500; and Karim Vellani, *Strategic Security Management: A Risk Assessment Guide for Decision Makers*, Elsevier, Oxford, 2007.

[69] For example, see: Karim Vellani, *Strategic Security Management: A Risk Assessment Guide for Decision Makers*, Elsevier, Oxford, 2007, p.28 ("Threat Formula", whereby "Threat = Intent + Capability + Motivation); and Peter Gasper, *Cyber Threat to Critical Infrastructure 2010-2015: Increased Control System Exposure*, Idaho National Laboratory, available at: http://usacac.army.mil/CAC2/CEW/repository/presentations/15_Idaho_Natl_Lab_IACS-CI_Threat_2010-2015.pdf accessed 4 Feb 2010 ("Threat = Capability + Intent + Opportunity).

assess the threat of a bioterrorist attack in the United States.[70] According to Pilch, vulnerability assessments are most effective where the potential target is specifically defined (e.g. the New York City subway system) rather than generic (e.g. the entire United States).[71] Nevertheless, Pilch adopts the generic referent of the United States against which to assess vulnerability, concluding that the United States is vulnerable to a bioterrorist attack. Pilch concludes his analysis by questioning whether the parameter of *capability* should be the single determiner of threat ("Conclusion: Threat = Capability?"). According to Pilch, as an open society, the US is vulnerable to a biological attack (thus *vulnerability* is a given) and *intent* cannot be accurately determined and therefore must be assumed.[72] As Pilch himself highlights, one of the weaknesses of the parameter of vulnerability is that the more generic the *potential* target (referent) the less insightful will be the assessment of threat.[73] At this stage, however, it is enough to demonstrate here that *vulnerability* is employed as an additional parameter to the dominant episteme, and that this parameter shifts focus onto the referent as opposed to the threat actor.[74] Nevertheless, vulnerability serves as an additional parameter, not as a break with the dominant episteme.

The parameter of *opportunity* also appears as an addition to the conventional model, such that *Threat = Intent x Capability x Opportunity*.[75] Unlike *vulnerability*, which is solely

---

[70] In this equation, Pilch defines vulnerability as "the extent to which a potential target is open to attack." Richard Pilch, The Bioterrorist Threat in the United States, in Russell Howard and Reid Sawyer (Eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004, p.208.
[71] *Ibid.*, p.211.
[72] *Ibid.*, p.233.
[73] *Ibid.*, p.211.
[74] A more detailed analysis of assessing potential *vulnerabilities* is included in Chapter 4.
[75] Defence Science and Technology Organisation, *Vulnerability and a High-Tech Adaptive Society*, presentation to the 2nd International Policing Conference, November 2004, available at: www.ipc2004.com/downloads/Scholz.pdf, accessed 30 November 2005. For the addition of opportunity as a parameter of threat (not in the form of an equation) see Alan Steinberg, Threat Assessment Technology Development, in Anind Dey, Boicho Kokinoc, David Leake, Roy Turder (Eds.), *Modeling and Using Context*, 5th International and Interdisciplinary Conference: Context 2005 Proceedings, Springer, Berlin,

focussed on an assessment of the referent, *opportunity* incorporates an understanding of both the threat actor and the referent. Opportunity can be defined as *a favourable time or occasion for a threat actor in relation to a referent*. The factor of opportunity relates to a time and space within which a target is able to be successfully attacked and is based upon a combination of circumstances of both a threat actor and a specific target or referent. The inter-relationship between the threat actor and the potential referent makes the parameter of opportunity inherently difficult to assess[76]; neither the threat actor nor the referent 'owns' opportunity. Instead, unlike the parameters of intent and capability (threat actor) and vulnerability (referent), assessments of opportunity relates to a space and time that exists outside or beyond both entities. As has been discussed, the nature and characteristics of non-state threats actually hinder such a clear definition of both the threat actor and referent (except at the most generic level). Without a detailed understanding of *both* the threat actor and referent, assessments of opportunity appear to be of limited use.

Extensions to Singer's model do highlight the complexity and multiple variables inherent in assessing threat. Nevertheless, whilst these extensions provide a more complex, and perhaps more rigorous, model of threat, whether such extensions bring clarity to assessing threat is an important question to ask. The act of simply adding parameters to the dominant episteme raises a legitimate question: How many parameters are enough? Whilst analysts might continue adding parameters as new aspects of threat are identified, at what point does adding parameters cease being useful? Indeed, where the threat actor or referent remain ill-defined, a greater number of parameters appears to increase rather than reduce the analytical complexities of threat assessment.

2005, pp.490-500.

[76] Eric Little and Galina Rogova, An Ontological Analysis of Threat and Vulnerability, in *9th International Conference on Information Fusion*, 10-13 July 2006, Figure 4.

One final observation is worth making. Despite attempts at broadening the dominant episteme to include the referent, the primary focus of assessments of threat remains tied to the threat actor. This is evident in that the parameters of vulnerability and opportunity are *extensions* to the existing parameters, not replacements. Thus, several assumptions are evident within attempts to extend the Singer's model:

- the model requires additional parameters to enable more complete understanding and assessment of threat;
- the parameters of *intent* and *capability*, and, therefore a principal focus on the threat actor, remain core; and
- the actor-based approach to understanding and assessing threat remains appropriate.

Despite efforts to incorporate additional parameters, the underlying assumption is that the dominant episteme with the primary focus on the threat actor remains central to assessing threat.

2.3 Methodology of Threat Assessment

Methodology:
A body of identifiable methods, rules and practices applied to a specific discipline. In this thesis, it is the methods used to make decisions about threat within the discipline of intelligence analysis.

With the dominant episteme of threat within the intelligence analysis field identified, it is

worth turning attention to the methodology used to inform assessments about the parameters of capability and intent. This section commences with a brief discussion on analysis, specifically the nature and characteristics of information that analysts use as the basis for decisions on state and non-state threats. The focus then moves to the measures, proxy-measures and indicators used for making decisions about state-based and non-state threats.

An intelligence analyst's role is to analyse and assess collected information in order to make judgements on actual or potential threats.[77] Intelligence agencies in the United States, Australia and the United Kingdom use all available sources of information to analyse and assess threats.[78] Consequently, these analysts use information collected through both classified means as well as information available through open (or public) sources. Examples of all-source information includes: "…satellite imagery, communications information, and human source reporting"[79], diplomatic reporting and open source material, such as news media, think-tank reports and academic publications.[80] Indeed, the information age has seen a near-exponential increase of global information meaning that intelligence analysts have been faced with what has been described as "a

[77] As a general rule, analysts tend not to be involved in the collection of information. Instead, analysts tend to be the *receivers* of information.

[78] For United States intelligence agencies, refer to Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005, p.9. For Australian intelligence agencies, refer to Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, Appendix 3 at:
http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/report/e03.pdf.
For United Kingdom intelligence agencies refer to Cabinet Office, *National Intelligence Machinery*, The Stationery Office, London, November 2006, p.39.

[79] George Tenet, Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee, 17 October 2002, p.10, at:
http://www.fas.org/irp/congress/2002_hr/101702tenet.pdf.

[80] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, Appendix 3 at:
http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/report/e03.pdf.

flood of information".[81]

The enormous volume of information collected by intelligence agencies, and their inability to digest, let alone analyse, all this information, is frequently acknowledged. According to McConnell, the United States intelligence community collects over one billion pieces of information every day.[82] Given this volume of information, it is little wonder that intelligence analysis has been likened to "trying to take a sip of water coming out of a fire hydrant".[83] Overwhelming amounts of information are a more recent phenomenon within intelligence, reflecting both advances in technology as well as an increased focus on potential non-state threats. Treverton argues that a challenge for analysis about state-based threats during the Cold War was that of too little information, "dominated by secret sources". In contrast, current non-state threats present analysts with the difficulty of too much information, a "broader range of sources, although secrets still matter".[84]

Evidence provided by analysts following successful mass-casualty attacks have consistently observed the overwhelming volume of information confronting them. The *Joint Inquiry into the Terrorist Attacks of September 11, 2001* notes that "[i]ndividuals in both the CIA and FBI units interviewed by the Joint Inquiry Staff reported being seriously overwhelmed by the volume of information and workload prior to September 11, 2001".[85]

---

[81] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.18 at:
http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/report/report.pdf.
[82] Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53.
[83] Louis Freeh, *Statement of Louis Freeh, Former FBI Director, before the Joint Intelligence Committees October 8, 2002*, p.8 available at:
http://www.fas.org/irp/congress/2002_hr/100802freeh.pdf accessed on 9 February 2010.
[84] Gregory Treverton, *Intelligence for an Age of Terror*, Cambridge University Press, New York, 2009, Table 1.1, p.2.
[85] Eleanor Hill, Joint Inquiry Staff Statement, Part 1, 18 Sep 2002, available at:
http://www.fas.org/irp/congress/2002_hr/091802hill.html accessed 8 Feb 2010.

Specific consideration of the CIA's Counter Terrorism Centre identified similar conclusions, with the Joint Inquiry Committee noting that "…within the CTC, the staff and resources dedicated to counterterrorism could not keep pace with the amount and scope of incoming intelligence reporting".[86] Similar observations were made by the Senate Committee investigating the 2002 Bali bombings. The Committee concluded that, before the bombings, "…analysts wrestled with what was becoming a flood of information to be interpreted, contextualised and assessed".[87] A comparable conclusion was reached by the Intelligence & Security Committee (ISC) following the 2005 London bombings. The ISC reviewed the work of the Joint Terrorism Analysis Centre (JTAC) before the attacks and observe that "[t]he volume of intelligence received on terrorist activity can be overwhelming, and difficult decisions have to be made as to what priority to accord a particular piece of intelligence and whether that piece or another lead should be pursued in more depth".[88] What is evident, therefore, is that an ability to collect vast quantities of information does not necessarily equate to an ability to analyse that information, let alone understand or accurately assess the relevance of such information. Neither does the ability to collect vast quantities of information necessarily indicate an ability to collect *relevant* information.

The nature and characteristics of collected information also impact on intelligence analysis. Lord Butler makes the observation that:

---

[86] US Senate Select Committee on Intelligence and US House Permanent Select Committee on Intelligence, Report of *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, December 2002, p.50 at: http://www.gpoaccess.gov/serialset/creports/911.html.
[87] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.18 at:
http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/report/report.pdf.
[88] Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006, p.7.

> The most important limitation on intelligence is its incompleteness. Much ingenuity and effort is spent on making secret information difficult to acquire and hard to analyse. Although the intelligence process may overcome such barriers, intelligence seldom acquires the full story. In fact, it is often, when first acquired, sporadic and patchy, and even after analysis may still be at best inferential.[89]

Thus, despite the enormous volume of information collected by agencies, the fragmentary and incomplete nature of available information makes comprehensive coverage of a topic rare.[90] The United Kingdom's Intelligence and Security Committee supports this conclusion, highlighting that intelligence "[a]gencies cannot know everything about everyone, nor can they intercept and read every communication (which in any event would be a gross violation of human rights). There will always be gaps in the Agencies' knowledge".[91] This observation is applicable to assessments of both state and non-state threats. For example, investigations into intelligence analysis on Iraqi WMD have acknowledged the limited amount of information available on WMD as well as the ambiguous and incomplete nature of the limited information which was available.[92] In relation to non-state threats, Manningham-Buller emphasises that "…intelligence rarely tells you all you want to know". Consequently, "[o]ften difficult decisions need to be made on the basis of intelligence which is fragmentary and difficult to interpret. In sum, some is gold, some dross and all of it requires validation, analysis and assessment".[93]

---

[89] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, p.14.

[90] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.8.

[91] Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006, p.7. See also Office of National Assessments Submission, *Security threats to Australians in South-East Asia*, Submission No.3, p.4 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub03.rtf.

[92] Refer to Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.107-109; also Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.34.

[93] Eliza Manningham-Buller, *Speech By The Director General of the Security Service, Dame Eliza Manningham-Buller, At The Ridderzaal, Binnenhof, The Hague, Netherlands*, 1 September 2005 available at: https://www.mi5.gov.uk/output/director-generals-speech-to-the-aivd-2005.html accessed on 11 February

The importance of the credibility of collected information has also featured heavily in recent inquiries. For example, in its submission to the Australian Senate Inquiry into the 2002 Bali bombings, the Defence Intelligence Organisation (DIO) argued that whilst there was a large amount of information on threats in South East Asia before the bombings, "…not all of the information was reliable".[94] Indeed, collected information can point analysts towards incorrect conclusions. Frank Lewincamp, the then Director of the Defence Intelligence Organisation, highlights that, before the attacks, most of the information being received by DIO indicated the likelihood of attacks elsewhere in Indonesia, namely on the island of Java some 250 kilometres away from the island of Bali.[95] Lewincamp also observed that "[m]uch of the information we receive is fragmented, it is uncorroborated, it is lacking in detail. In fact, in many cases it is contradictory. So this requires the application of careful judgment, and judgments between analysts, very skilled analysts, will often differ".[96] The idea that different analysts can interpret the same information differently was highlighted by Rear Admiral Jacoby, Acting-Director of the Defense Intelligence Agency. Jacoby observed that "[i]nformation considered irrelevant noise by one set of analysts may provide critical clues or reveal significant relationships when subjected to analytical scrutiny by another".[97] Nonetheless, regardless of the ambiguity or contradictory nature of information, analysts are still required to make decisions about state-based and non-state threats. As Wright-Neville

---

2010.

[94] Defence Intelligence Organisation, Department of Defence, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 28 May 2004, p.8 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/qon/dio_qons.pdf.

[95] Frank Lewincamp, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.348 at: http://www.aph.gov.au/hansard/senate/commttee/S7207.pdf.

[96] Frank Lewincamp, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.55-56 at: http://www.aph.gov.au/hansard/senate/commttee/S6557.pdf.

[97] Lowell Jacoby, *Statement for the Record for The Joint 9/11 Inquiry: Information Sharing of Terrorism-Related Data*, 1 October 2002, p.4, available at: http://www.fas.org/irp/congress/2002_hr/100102jacoby.pdf accessed on 11 February 2010.

observes "[a] good analyst has to try and piece together imperfect information to make a judgement on what is likely to happen in the future".[98] Having briefly looked at the nature and characteristics of information used by analysts, and the complex undertaking that is intelligence analysis, the next section discusses how analysts reach decisions about state's capabilities and intentions as part of broader assessments of threat.

The parameter of *capability* is central to current understanding of threat. Despite this, definitions of *capability* are regularly absent from intelligence analysis, presumably based on the assumption that *capability* is clearly understood or self-evident. The assumption that *capability* is understood and consistently applied is questionable. Sherman Kent, a prominent US figure in the study of intelligence analysis during the Cold War, identifies this very issue when outlining the requirement for an intelligence literature. Kent observes that, whilst the term *capability* is arguably used by analysts more than any other semi-technical word, it is used indiscriminately to mean one of three different things: a feasible course of action, a raw strength, or a talent or ability. Kent's concern was that analysts could not be certain that they were always conveying their intended meaning of the word.[99]

Where *capability* is deliberately defined, the meaning of the term can be either generic or specific. That is, the parameter *capability* can be defined either at the broadest level to assess a state's overall military capability or more specifically to assess a *type* of capability. For example, definitions included within declassified intelligence include

[98] David Wright-Neville, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 November 2003, p. 257 at: http://www.aph.gov.au/hansard/senate/commttee/S7205.pdf.
[99] Sherman Kent, *The Need for an Intelligence Literature*, CIA Center for the Study of Intelligence, available at:https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/sherman-kent-and-the-board-of-national-estimates-collected-essays/2need.html accessed 11 February 2010.

assessments of a state's overall capability to conduct "combat operations".[100] Conversely, the term is also defined to focus on a particular type of capability, for example a state's nuclear development capability.[101]

It can be argued that analysts use two approaches for assessing capability. These are the use of *measures* and *proxy-measures*. A measure can be defined as *a definitive unit or quantity which enables a direct assessment of capability*. In comparison, proxy-measures are factors used to draw conclusions about *capability* where direct measures are not observable. Thus, a proxy-measure can be defined as *an indirect measure used to make inferences about capability*.

Measure:
A definitive unit or quantity which enables a direct assessment of capability.

Proxy-measure:
An indirect measure used to make inferences about capability.

A measure is directly linked to capability, enabling an analyst to make a decision about capability. As states attempt to maintain uncertainty over their actual capabilities and even develop clandestine capabilities, direct measures can be disguised or hidden. Where measures are not observable, proxy-measures are used, but only to *infer* capability. Nevertheless, states cannot entirely disguise their capabilities, as is evident with the

[100] National Intelligence Council, *Iraqi Military Capabilities Through 2003*, NIE 94-19, July 1994, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[101] National Intelligence Council, *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007, available at http://www.dni.gov/press_releases/20071203_release.pdf accessed on 15 February 2010.

example of the Soviet nuclear capability (see following). Indeed, states deliberately make some measures of capability visible in order to deter or influence other states. Consequently, assessments of state capabilities are usually based upon both measures and proxy-measures.

Soviet Nuclear Capability: Measures and Proxy-Measures

During the Cold War, much of the focus of United States and United Kingdom's intelligence agencies was on the analysis of the Soviet Union's nuclear weapons capability. As much of this early analysis in now declassified, these assessments provide a good example of the use of measures and proxy-measures in assessing a particular type of capability.

Measures

The CIA's *National Intelligence Estimate: Soviet Capabilities and Intentions* (November 1950), illustrates several measures used to assess Soviet nuclear capability: total number of atomic bombs; delivery mechanisms (aircraft; trained aircrew; bases of operation; guided missiles; submarines); and scientific development.[102] Additionally, fissionable materials and nuclear reactor programs were also measures.[103] However, strict security practices and the clandestine nature of much of the Soviet's efforts ensured that many of these measures were not directly observable.[104]

[102] Central Intelligence Agency, *Soviet Capabilities and Intentions*, National Intelligence Estimate 3, 15 November 1950, in Scott Koch (Ed.), *CIA Cold War Records: Selected Estimates on the Soviet Union 1950-1959*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 1993, p.172.
[103] Director of Central Intelligence, *The Soviet Atomic Energy Program*, National Intelligence Estimate 11-2A-63, 2 July 1963, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[104] Central Intelligence Agency, *Intelligence Aspects of the "Missile Gap"*, November 1968, p.13, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.

Proxy-measures

A now declassified CIA review into the "missile gap crisis" provides an insight into the proxy-measures which were used to assess Soviet nuclear weapons capability, specifically the Inter-Continental Ballistic Missile (ICBM) nuclear capability.[105] The proxy-measures used to infer capability included: Soviet missile test range activities; limited U-2 imagery of facilities; the launch of Sputnik (as a measure of technical progress); the USSR's curtailed build-up a bomber force (assuming the efforts had moved to ICBM development instead); the US' own progress in the development of nuclear weapons; and analysis of Soviet leaders' statements on the scale of ICBM production.[106] In 1961, "regular satellite photography" provided detailed imagery of more proxy-measures (ICBM testing complexes and the Soviet rail network) as well as enabling some direct measures to be observed (e.g. aircraft, submarines, missile launchers and missiles).[107]

Singer's concept of capability was based on a state's military power, in particular military (principally nuclear) weaponry.[108] In this respect, Singer's work is similar to measures of capability evident within declassified intelligence. As Bennett argues, the focus on similarly-balanced state-based threats "…led many US analysts to conclude that quantitative measures of military hardware, units, and warfighters were the key metrics for evaluating the military capabilities".[109] The advent of satellite imagery also served to

[105] *Ibid*.
[106] *Ibid.*, pp.14-17.
[107] *Ibid.*, p.32.
[108] According to Singer, the "…exacerbation of mutually ominous military capabilities…" is recognised by policy-makers in the US and USSR recognise that each "…has at its disposal an array of weapons and delivery systems". This is evident in Singer's definition of *disarmament* as "…the reduction of a nation's military capabilities". J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.
[109] Bruce Bennett, Responding to Asymmetric Threats, in Stuart Johnson, Martin Libicki and Gregory Treverton (Eds.), *New Challenges, New Tools for Defense Decisionmaking*, RAND Corporation, Santa Monica, 2003, pp.33-66, p.35.

enforce a focus on military weapons as a primary measure of capability. By the early 1960s, satellite technology enabled the US Defence Intelligence Agency (DIA) and CIA to "…find, count, and describe any piece of large-scale military hardware on or near the surface of the earth".[110] This had an impact of the confidence of both analysts and decision-makers in assessments of Soviet capabilities. President Johnson, when discussing Soviet nuclear weapons, is quoted observing that "[b]ecause of the satellites, I know how many missiles the enemy has".[111] Indeed, by the 1990s, the effectiveness of satellite and electronic collection led one commentator to observe that "…measuring capability is a very concrete art".[112] Indeed, it is perhaps not surprising that, in at least some instances, capability has been used to denote little more than weapons and orders-of-battle. For example, Frank Stech, writing in 1979, observes that "[a]n increasingly common usage of "capabilities" connotes nothing more than the number of weapons of various kinds. This is an unfortunate simplification of the term since the possession of a weapon by no means denotes a particular capability with it. However, in modern usage weapons inventories are frequently used to denote capability".[113] The focus on standing armies and military hardware is evident in declassified intelligence analysis. For example, the CIA's 1977 report, *The Balance of Forces in Central Europe*, estimates Soviet and Warsaw Pact armed force capabilities based on the total numbers of: armed force personnel; tanks; armoured vehicles; artillery; tactical aircraft; and tactical nuclear weapons. These estimates were contrasted directly against the numbers of corresponding US/NATO personnel and

[110] Thomas Powers, *Intelligence Wars: American Secret History from Hitler to al-Qaeda*, New York Review Books, New York, 2004, p.398.
[111] Stephen Beitler, Imagery Intelligence, p.79, in Michael Herman, *Intelligence power in peace and war*, Cambridge University Press, Cambridge, 1996, p.74.
[112] David Snow, *National Security: Enduring Problems in a Changing Defense Environment*, 2nd Edition, St Martin's Press, New York, 1991, p.246.
[113] Frank Stech, *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of National Research, November 1979, p.21.

weaponry.[114] The use of total numbers of both military weapons and armed forces personnel as measures of capability has remained consistent. The National Intelligence Council's 1999 assessment of *Iraqi Military Capabilities Through 2003*, highlights the ongoing focus on total numbers of military weapons and armed forces personnel as measures of capability.[115] This is not to suggest that capability assessments focussed solely on total numbers of weapons or personnel. Qualitative measures of combat capability are also included throughout these two reports (e.g. fighting ability, training, morale and leadership). Nevertheless, the central focus on total numbers of military weapons and personnel indicates their prominence as a measure of a state's capability.

The breakthrough with satellite imagery did provide governments with a tool for measuring capabilities based on military equipment. However, satellites can only image what is observable and not concealed, thus imagery might only provide proxy-measures or clues for assessing capability.[116] Consequently, imagery assessments are open to interpretation, and it does not necessarily follow that capability will be correctly assessed. Two cases involving the public use of imagery as evidence of capability are worth considering. On 25 October 1963, the United States Ambassador to the United Nations, Aldai Stevenson, famously displayed U-2 imagery as evidence that the USSR had deployed missiles to Cuba. In same forum, almost forty years later, Secretary of State Colin Powell also used satellite imagery to make the case of the presence of WMD within Iraq. Given the very different outcomes of these two situations, imagery alone is clearly no guarantee of evidence of state-based capabilities. Further, despite the use of "satellite and

[114] Central Intelligence Agency, *The Balance of Forces in Central Europe*, August 1977, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[115] National Intelligence Council, *Iraqi Military Capabilities Through 2003*, NIE 94-19, July 1994, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[116] Michael Herman, *Intelligence power in peace and war*, Cambridge University Press, Cambridge, 1996, p.76.

electronic collection"[117], the debate over the *accuracy* of capability assessments (particularly those of the Soviet Union) continues.[118] It is evident in both US intelligence reports cited above that not all weapons or personnel were directly observed. The fact that the number of Iraqi and Soviet/Warsaw Pact personnel and weapons are rounded off to the nearest ten (combat aircraft, artillery), hundred (tanks), or thousands (personnel) illustrates the estimative nature of these numbers. Thus, assessments of the total number of armed force personnel rely on both measures and proxy-measures. Even so, a state's weaponry and armed forces (where accurately assessed) provide a relatively stable measure for analysts and decision-makers, enabling a degree of confidence in assessments of current and future military capabilities.[119]

While military weapons and armed forces are measures of capability, they are clearly not the only measures. Simply because a state has certain military weaponry does not mean that this weaponry can be used effectively. Neither does it follow that a state could draw upon the total number of armed personnel to fight as expected. Therefore, other measures are required to provide a comprehensive understanding of military capability. In outlining doctrine for conducting Military Capability Assessments, the US' *Joint and National Intelligence Support to Military Operations* highlights the range of measures and proxy-measures used. According to the publication, there are five direct measures for assessing

[117] David Snow, *National Security: Enduring Problems in a Changing Defense Environment*, 2nd Edition, St Martin's Press, New York, 1991, p.246.

[118] Decades after the fall of the Soviet Union, Rolington observes that during the Cold War "…hundreds of Soviet weapons capability reports were produced, but it is now recognised that most were extremely wide of the mark, with the Soviet threat over-estimated by an average of two to one". Alfred Rolington, Keeping intelligence objective, *Jane's Intelligence Review*, 01 December 2005, accessed on-line by subscription., Lowenthal argues differently, stating that "[a]lthough the US intelligence community made mistakes, such as overestimating and underestimating missile forces, overall Soviet capabilities were fairly well known in detail". Mark Lowenthal, *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006.

[119] This stability is due in large part to the significant financial, material and personnel costs that states invest in military weaponry and armed forces. States' industrial-scale production of weapons and compulsory military service during time of war (e.g. World War Two) are an exception to this relative predictability.

military capability: leadership and C2 (command and control); order-of-battle; force readiness and mission; force sustainability; and technical sophistication.[120] Additionally, proxy-measures (titled military related subjects assessment) are provided, including: C4 systems (telecommunications and networks); the state's Defence industries; energy/power; geography; demography; and medical capability.[121] This list illustrates that there are potentially innumerable measures and proxy-measures, depending upon the level of specificity and type of capability being assessed.[122] A final observation by the UK's Joint Intelligence Committee is telling. In a 1948 analysis the JIC observed that "[t]he comparative fighting value of Russian and Allied armed forces will vary according to the nature of particular operations".[123] This raises the idea that, despite identifiable measures and proxy-measures, capabilities are actually contextual. Consequently, state-based capabilities might only be knowable once they are actually used against an opposing force.

As detailed in section 2.1, the nature and characteristics of state and non-state threats differ significantly. Therefore, the measures and proxy-measures for assessing state capabilities are not necessarily applicable for assessing non-state capabilities. Wastell *et al* capture this point, when they argue that "[i]ntelligence assessments during the Cold War revolved around examining the balance of capabilities (e.g., tanks, submarines and missiles). Such an assessment now against terrorist groups is at best misguided and at worst delusional".[124] The measures and proxy-measures used to assess non-state capabilities will be discussed in

[120] Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication JP 2-01, October 2004, p.III-40.
[121] Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication JP 2-01, October 2004, pp.III-40-41.
[122] For example, Tellis *et al*. list 96 measures for assessing a military's ground warfare capabilities. Ashley Tellis et al., Janice Bially, Christopher Layne, Melissa McPherson, Jerry Sollinger, *Measuring National Power in the Postindustrial Age*, RAND Corporation, Santa Monica, 2000, pp.162-163.
[123] JIC(48)76, para 1, quoted in Alexander Craig, *The Joint Intelligence Committee and British Intelligence Assessment, 1945-1956*, unpublished PhD thesis, July 1999, p.76.
[124] Colin Wastell, Graeme Clark, and Piers Duncan, Effective Intelligence Analysis: The Human Dimension, *Journal of Policing, Intelligence and Counter Terrorism*, Vol.1, October 2006, pp.36-52, pp.37-38.

detail in Chapter 3, with contrasts between assessments of state-based capabilities highlighted.

Singer's understanding of intent could be described as a state hierarchy's military designs towards another state.[125] This is similar to the context with which Sherman Kent appears to use the term in describing the CIA's misunderstanding of "Soviet intentions" prior to the Cuban missile crisis.[126] The difficulty with the term *intent* is that, similar to *capability*, definitions of *intent* are notably absent despite the frequent use of the term in describing threat. Again, the absence of definitions of intent is presumably based on the assumption that the term is clearly understood or self-evident. However, as demonstrated in the examples below, where defined, it is apparent that intent is interpreted differently.

The Australian Department of Defence described intentions "…the adversary's decisions and policies, in the context of national values and institutions".[127] This is reflected in Huntington's discussion of a state's intentions as political in nature, being reflected in the state's policies.[128] Coral Bell's appears to make a similar argument when describing the more predictable nature of states, in contrast to non-state actors, noting that that it is diplomats who attempt to determine states' intentions.[129] Constantine FitzGibbon argues that states' strategic intentions are publicly reflected in the publications and statements of state leaders, consequently the idea is that state intentions are "underlined" and "made

[125] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.95.
[126] Sherman Kent, *A Crucial Estimate Relived*, Center for the Study of Intelligence, accessed on 10 March 2011 at: www.cia.gov/
[127] Department of Defence, *Australia's Strategic Planning in the 1990s*, Departmental Publications, Canberra, September 1989, p.24.
[128] Samuel Huntington, *The Soldier and the State: The Theory and Politics of Civil-Military Relations*, Vintage Books, New York, 1957, pp.66-67.
[129] Carol Bell, *Living with giants: Finding Australia's place in a more complex world*, Australian Strategic Policy Institute, Barton, 2005, p.20.

abundantly clear".[130] But this sits uncomfortably with Lowenthal's description of intentions as "…the plans and goals of the adversary…" which, compared with capabilities, "…are a more amorphous subject and pose a much more difficult collection problem".[131] The US Joint Chiefs of Staff definition of intent is more specific than those above, referring to "[a]n aim or design (as distinct from capability) to execute a specified course of action".[132] The ASIO definition of intent is similarly as "…the desire of a subject to cause harm and its own confidence in its capacity to do so".[133] Thus, as discussed with the parameter of *capability*, intent can be defined broadly or specifically. At the broadest level, intentions can be defined as the overall goals and aims of a state or leader. More specific definitions might relate to the state's plans over a particular issue, for example Iran's intentions to develop a nuclear weapons capability.[134]

The very nature of an intention means that it is not 'measurable' like capability.[135] Whilst capabilities can be measured *externally* to individuals, intentions are essentially an individual's or a group's *internal* decisions. As intentions are internal to an individual or group, they are estimated or inferred from observable factors, termed *indicators*.

---

[130] Constantine FitzGibbon, *Secret Intelligence in the Twentieth Century*, Hart-Davis MacGibbon, London, 1976, p.334.
[131] Mark Lowenthal, *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006, p.223.
[132] Joint Chiefs of Staff, *Joint Intelligence*, Joint Publication 2-0, Washington, D.C., 22 June 2007.
[133] Australian National Audit Office, *Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games*, Commonwealth of Australia, Canberra, August 1998, p.66.
[134] National Intelligence Council, *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007, available at http://www.dni.gov/press_releases/20071203_release.pdf accessed on 15 February 2010.
[135] In comparing intelligence analysis with the scientific method, Isaac Ben-Israel argues that "[i]n intelligence, unlike science, we have to estimate intentions". Isaac Ben-Israel, Philosophy and Methodology of Intelligence: The Logic of Estimative Process, *Intelligence and National Security*, Vol.4, No.4, October 1989, pp.660-718, p.691.

Indicator:
An observable factor used to infer or estimate current or future intentions.

In the case of assessing a state's intentions, it is the intentions of the state's leaders that are the focus of analysis. If these leaders' internal intentions are to be acted upon, then the articulation of, or actions reflecting, these intentions potentially provide observable indicators. Nevertheless, these indicators provide a means to infer rather than quantify. The less-quantifiable nature of intentions is perhaps why intelligence agencies have had less confidence in assessing state intentions over state capabilities.[136] The difficulty in assessing intentions has been addressed by a number of researchers[137], and there has been debate over whether or not an individual's intentions are knowable. For example, Butler argues that, just like an enemy's order-of-battle an enemy's intentions are knowable[138], whereas Richard Best claims that foreign leaders' intentions are a "mystery" and are therefore not knowable.[139]

There are three indicators which feature prominently in assessments of state intentions, namely: assessments of state's military capability; state ideology; and assessments of the

[136] For example, the CIA report, *Warning of War in Europe*, argues that the US warning system "…can assess potentially enemy capabilities; it is less reliable for forecasting hostile intent, which might become apparent only in the act of war itself". Central Intelligence Agency, *Warning of War in Europe*, June 1984, p.3, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[137] Refer to Constantine FitzGibbon, *Secret Intelligence in the Twentieth Century*, Hart-Davis MacGibbon, London, 1976, p.334; Mark Lowenthal, *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006, p.223; and Walter Laqueur, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, 1993, p.23; and Isaac Ben-Israel, Philosophy and Methodology of Intelligence: The Logic of Estimative Process, *Intelligence and National Security*, Vol.4, No.4, October 1989, pp.660-718, p.691.
[138] Refer to Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.14-15.
[139] Richard Best, *Intelligence Issues for Congress*, Congressional Research Service, Library of Congress, 9 May 2006, available at: http://www.fas.org/sgp/crs/intel/IB10012.pdf accessed on 16 February 2010.

words, actions and behaviour of state leaders. These are each reflected in Singer's work. Most immediately apparent in Singer's description is the assessment of military capability. According to Singer, "…each elite will interpret the other's military capability as evidence of military intent".[140] This is based upon the perception that decision-makers will err on the side of cynicism and assume hostile intentions based on military hardware because of the potentially disastrous consequences for the state.[141] Again, Singer's observation is reflected in declassified intelligence assessments. For example, according to the United States' 1982 National Intelligence Estimate, *The Soviet Challenge to US Security Interests*, the expansion and modernisation of Soviet military capabilities "…demonstrates Moscow's intention of dominating the regional military balances in Central Europe and along the Sino-Soviet frontier".[142] Additionally, the movement and preparation of military forces was also seen as "…the least equivocal events leading to war readiness, and would constitute the principal events upon which [intelligence] warnings would be based".[143] In her review of the attack on Pearl Harbour, Wholstetter concluded that US intelligence agencies "…lacked the data on enemy intentions deduced from the movements of forces".[144] Consequently, military weaponry and armed forces are used both as a measure of a state's military *capability* and an indicator of state *intentions*. However, as Singer himself demonstrates, assessments of military capability alone are not enough to infer a

[140] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.
[141] *Ibid.*, p.94.
[142] Central Intelligence Agency, *The Soviet Challenge to US Security Interests*, National Intelligence Estimate 11/4-82, p.3.
[143] Central Intelligence Agency, *Warning of War in Europe*, June 1984, p.4, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[144] Roberta Wohlstetter, *Pearl Harbour: Warning and Decision*, Stanford University Press, 1962, p.364. Nevertheless, even where intelligence agencies collect information on the movement of military forces, it does not mean that intentions will be accurately assessed. The 1973 Egyptian preparations for the Yom Kippur War and the 1991 Iraqi preparations for the invasion of Kuwait offer two examples of intelligence agencies having information on the deployment of armed forces but misinterpreting the purpose of the build-ups.

state's intentions.[145]

Singer acknowledges that despite the United Kingdom having a "formidable military establishment" the UK is not a threat to the United States.[146] As noted earlier, forty years later, Richard Betts made this argument over nuclear threats, similarly using Britain as an example. Betts argues that "both Britain and France have the capability (in their SLBM warheads) to incinerate several dozen American cities, but US warning officers spend no time at all worrying about this because they know that there is no intention in London or Paris to do this".[147] Thus, indications of intent are both a state's military establishment as well as the ideology of the state's hierarchy. The assumption of hostile intentions of states with a Communist ideology is evident in the consistent focus on Communist states by intelligence agencies in the UK, US and Australia during the Cold War. Two examples are worth citing. The influential NSC-68 emphasised the ideological conflict "…in the realm of ideas and values between the US purpose and the Kremlin design".[148] Some thirty four years later, the US National Intelligence Estimate, *The Soviet Challenge to US Security Interests*, similarly noted that "…ideological antagonism and geopolitical rivalry, governs Soviet behaviour and shapes Soviet perceptions of US policies towards Moscow".[149] United States analysts' perceptions of Soviet ideology influenced their assessments of Soviet intentions. Of course, a state's ideology is a reflection of the political leadership, the third indicator of intentions.

---

[145] J. David Singer, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105, p.94.
[146] *Ibid.*, p.94.
[147] Richard Betts, Intelligence Warning: Old Problems, New Agendas, *Parameters*, Spring 1998, pp.26-35.
[148] National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950.
[149] Central Intelligence Agency, *The Soviet Challenge to US Security Interests*, National Intelligence Estimate 11/4-82, p.1, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.

The focus on well-defined political and military hierarchies in order to assess state intentions is evident within declassified intelligence analysis. Indeed, an often singular focus on the state's leadership is evident in how states are often referred to by their capital city or political office.[150] More specifically, assessments of state intentions often focus on a single individual, namely the most senior political leader.[151] As evident in the Butler review, assessments of Iraqi intentions were based on an assessment of Saddam Hussein himself. Indeed, the lack of access to those closest to Hussein was seen as a severe limitation in accurately assessing Iraqi intentions.[152]

In determining state intentions, it is the words (spoken or written) of the state's leadership that are analysed. For example, the analysis of *Soviet Short-Term Intentions Regarding Berlin and Germany* based assessments of intentions on "Soviet public and private statements".[153] Private statements can be obtained through face-to-face meetings between state leaders, with analysts using these discussions as the basis for updating assessments of state intentions and identifying changes and shifts in intentions.[154] Meanwhile, public speeches are also used to assess intentions. The 1963 assessments of the Soviet military's

[150] For example, the USSR is regularly referred to as 'the Kremlin' and 'Moscow'. Refer to Central Intelligence Agency, *Soviet Short-Term Intentions Regarding Berlin and Germany*, National Intelligence Estimate 11-7-61, pp.2-3, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[151] Richard Aldrich, *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*, The Overlook Press, Woodstock, 2001, p.62.
[152] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.75, 83 & 165.
[153] Central Intelligence Agency, *Soviet Military Capabilities and Policies, 1962-1967*, NIE-11-4-63, March 1963, p.2, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[154] For example, refer to Central Intelligence Agency, *Soviet Foreign Policy in the light of the Summit Conference*, National Intelligence Estimate 11-13-55, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010. The report observes that "[w]e conclude that the Soviet leaders have not abandoned their long-range aims. During the current phase, however, they have embarked on a policy aimed at a general easing of cold was tensions". p.5.

future priorities were influenced by Khrushchev's public speeches, taken as indicating Soviet leadership decisions.[155] The absence of information on (or lack of access to) state leaders underscores the reliance on the words and behaviours of state leaders in assessing state intentions. In its 1946 report, *Russia's Strategic Interests and Intentions*, the United Kingdom Joint Intelligence Committee acknowledged at the outset of the report that assessments of Russian intentions were largely speculative due to the lack of access to, and intelligence on, Russian leadership.[156]

Singer's own work and declassified intelligence assessments enable the identification of measures, proxy-measures and indicators used to assess state's capabilities and intentions. The next chapter explores the measures, proxy-measures and indicators used to assess non-state actors' capabilities and intentions.

[155] Central Intelligence Agency, *Soviet Military Capabilities and Policies, 1962-1967*, NIE-11-4-63, March 1963, p.5, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.
[156] JIC(46)1, 1st March 1946, *Russia's Strategic Interests and Intentions*, para 3, CAB81/132, PRO, quoted in Alexander Craig, *The Joint Intelligence Committee and British Intelligence Assessment, 1945-1956*, unpublished PhD thesis, p.23.

Chapter 3

A Critique of Singer's Model as Applied to Non-State Actors: The Intangibility of Capability and Intent

3.1 Measures, Proxy-measures and Indicators of Capability and Intent

The parameters of intent and capability are valuable only insofar as they provide an insight into threat, and that they are based upon observable indicators, measures and proxy-measures. The importance of being able to observe these parameters is evident in the United States' *National Strategy for Homeland Security* which argues that intelligence agencies "…must identify, collect, and analyze the new observables that will enable us to better understand emerging unconventional threats".[1] This quote also suggests that a change in the focus from state-based to non-state threats results in new, or at least different, observable measures and indicators. Thus, whilst basing assessment on the same episteme of threat, there are differences in how analysts arrive at assessments of non-state vice state-based threats. This chapter will evaluate state-based measures, proxy-measures and indicators as applied to assessing non-state capabilities and intentions with regard to mass-casualty attacks.

3.2 Measuring the Capability to conduct a mass-casualty attack

As discussed in Chapter 2, non-state actors do not necessarily rely on standing armies or large-scale military weaponry to project killing power. Numerous mass-casualty attacks conducted by non-state actors have not required either large-scale military weapons or the

[1] Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.16.

use of standing armed forces. Instead, attacks like those in Madrid (2004) and Mumbai (2008) have demonstrated that non-state actors can project mass-killing power without resorting to large-scale military capabilities usually associated with state-based threats. These attacks raise questions over the applicability of state-based measures for assessing non-state capabilities. It can be said with a certain degree of confidence, whether or not a state lacks a capability to successfully attack another state.[2] However, it is difficult to claim that a non-state actor is *incapable* of carrying out a mass-casualty attack given the diversity of available tools that can be used to conduct a successful attack.

Arguably, the greatest concern of analysts and decision-makers in terms of non-state threats is a mass-casualty attack using WMD.[3] This concern existed prior to the 11 September 2001 attacks. In 1998, CIA Director, James Woolsey testified that the risk of WMD by terrorists represented "…the number one threat to our national security".[4] WMD is generally associated with chemical, biological, radiological and nuclear (CBRN) technologies.[5] The ongoing debate over just how difficult it is for a non-state actor to acquire, develop or use WMD in a mass-casualty attack, hinting at the difficulty of unambiguous measures of WMD capability.[6] The debate is also reflective of the diverse range of potential weapons and technologies included under the broad heading of WMD. Nonetheless, there is an argument that, due to the spread of knowledge, technology and

[2] This is not to suggest that assessing another state's *capabilities* is analytically straightforward, as recent history indicates that this is clearly not the case. Intelligence over Iraq's WMD *capability* and ongoing debate about Iran's nuclear *capability* are two examples.
[3] Sloan argues that WMD terrorism dominates contemporary security debate in both official and academic circles in North America. Elinor Sloan, *Security and Defence in the Terrorist Era: Canada and North America*, McGill-Queen's University Press, Montreal, 2005, p.28.
[4] Testimony of R. James Woolsey, US House of Representatives Committee on National Security, February 12, 1998.
[5] Of interest, the United Kingdom Counter-Terrorism Strategy broads the definition of CBRN to also include *explosives*, refering more broadly to the "CBRNE threat". United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.11.
[6] For example, refer to Stratfor, *The Jihadist CBRN Threat*, 10 February 2010.

materials, the opportunities for non-state actors to gain WMD capabilities are increasing.[7] Therefore, it is worth briefly examining the ease or difficulty for developing WMD and considering the measures and proxy-measures upon which assessments of WMD capabilities are based. The purpose here is to provide a generic overview of the perceptions of the ease or difficulty for analysts attempting to assess the various types of WMD which non-state actors could potentially use. It is not an attempt to describe *in detail* the technical, material or knowledge requirements to produce each of these types of weapons. This is beyond the scope of this thesis as such efforts would reflect entire *fields* of research.

Developing a nuclear weapons capability is not an easy undertaking, even for states. Consequently, there is general agreement that it would be extremely difficulty (if not impossible) for non-state actors to develop a nuclear weapons or employ nuclear weapons to conduct a mass-casualty attack. In a review of the literature on nuclear terrorism, Daniel Gressang highlights that the most frequently cited deterrent is the sheer weight of technical and material demands required to develop and manufacture nuclear weapons including: capital expenditure; high technology machining equipment; facilities infrastructure; and a suitable and secure location.[8] The scale of technical demands makes it likely that the measures and proxy-measures Gressang identifies would be observable to analysts looking to confirm the *development* of nuclear weapons by a non-state actor.

The perception of the extreme difficulties for non-state actors attempting to develop a nuclear weapons capability has resulted in states focussing their efforts on preventing non-

[7] Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.9.
[8] Daniel Gressang, Audience and Message: Assessing Terrorist WMD Potential, in Alan O'Day (Ed.), *Weapons of Mass Destruction and Terrorism*, Ashgate, Aldershot, 2004, pp.86-87.

state actors from *acquiring* nuclear weapons or weapons-grade uranium and plutonium by securing states' nuclear weapons and materiel.[9] Thus, in terms of observable proxy-measures for a nuclear weapons capability, the focus appears to be on *acquisition* rather than development.[10] The measures for a non-state actor's nuclear weapons capability would appear to be the weapons themselves and the means to acquire and detonate them. Proxy-measures would appear to be: access to state-nuclear weapons; funds to illegally purchase weapons and materiel; and resources to move and store the weapon. Whilst analysts remain concerned by the potential for non-state actors to acquire already nuclear weapons, efforts to monitor and control existing state weapons have increased confidence in measures and proxy-measures.

There is disagreement over the challenges facing non-state actors attempting to develop a chemical or biological weapons capability.[11] These differences of opinion provide an insight into the difficulty of identifying unambiguous measures and proxy-measures of both the development and acquisition of chemical and biological weapons capability.

The equipment, information and materiel to develop chemical weapons are not only relatively inexpensive, but can be difficult to delineate from non-threatening activity. Chemical weapons themselves are a measure of capability. Beyond identifying the actual weapons, analysts rely on proxy-measures, which are inherently ambiguous. In considering

[9] Bob Graham et al., *World At Risk:The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, Vintage books, New York, pp.43-44. Recently, there have been concerns raised over the potential for Pakistan's nuclear weaponry to fall into the hands of non-state actors if the Taliban took control of the country.

[10] More recently, there have been concerns raised over the potential for Pakistan's nuclear weaponry to fall into the hands of non-state actors if the Taliban took control of the country.

[11] Whilst acknowledging significant differences between chemical and biological weapons, within the intelligence literature analysis of the ease or difficulty of developing a chemical or biological weapon is regularly included under the same broad heading. Thus, references within the chemical and biological weapons will, at times, refer to both in the same sentence.

the difficulty facing intelligence agencies attempting to address unconventional or asymmetric threats, *Jane's Information Group* argued that the proliferation of chemical and biological weapons is due to the small cost, ease of development and availability of material.[12] Accurate assessment of a chemical weapons capability is hampered by the "dual-use" of technology used to produce them.[13] The equipment and materials used to make chemical weapons "…include items such as fermenters, aerosol generators, protective gear, antibiotics, and disease-causing agents [which] have not just terrorist applications, but also legitimate commercial applications, and can often be bought on the open market".[14] This presents a dilemma for analysts in that these measures and proxy-measures of chemical weapons capability could also be evidence of non-threatening behaviour.

The use of chemical weapons by some non-state actors has also been taken as a proxy-measure of their potential use by other non-state groups. This view is reinforced by Krahmann, who argues that actual attacks, namely the sarin attacks conducted by Aum Shinrikyo in Tokyo in 1995, illustrate the "…relative ease with which chemical agents can be manufactured by amateurs".[15] There has, however, been a counter-argument that Aum's failure to perpetrate a true-mass casualty WMD attack, despite significant financial outlay, infrastructure and years of preparation, has implications for WMD potential of groups like

---

[12] Kevin O'Brien, Intelligence Gathering on Asymmetric Threats - Part One, Jane's Intelligence Review, Vol. 12, No.10, October 2000, pp. 50-55, p.55.

[13] *Ibid.*, p.55. Rather than 'dual-use', technology is probably better described as 'multi-use', with many alternative uses often identified only once the technology has been commercialised or made publicly available.

[14] Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.17-18.

[15] Elke Krahmann, From State to Non-State Actors: The Emergence of Security Governance, in Elke Krahmann (Ed.), *New Threats and New Actors in International Security*, Palgrave MacMillan, New York, 2005, p.4.

Al Qa'ida.[16] Regardless, even where reporting is received, and the group identified by intelligence agencies as a threatening entity, confirmation of a chemical weapons capability might not be achievable without having direct access to the group and their resources. Salam and Hansell discuss the myriad of reports of Al Qa'ida producing chemical and biological weapons that were received before October 2001. They highlight that it was only once United States armed forces gained physical access to Al Qa'ida bases in Afghanistan that it became apparent, based upon the group's resources, that that Al Qa'ida were far from developing a true chemical weapons capability.[17] Thus, it would appear that attempts to achieve an unambiguous assessment of chemical weapons capability appears problematic without direct access to the group itself, which is not guaranteed.

In considering biological weapons capability, the United States' *Commission on the Prevention of WMD Proliferation and Terrorism* acknowledged the difficulty in identifying unambiguous measures or proxy-measures of non-state actors developing a biological weapon. The Commission argued that the development of biological weapons can "…easily be concealed within a host of legitimate activities, such as pharmaceutical development, vaccine production, and general life sciences research".[18] Consequently, confirmation of a biological weapons capability is difficult to quantify.[19]

Basing measures of a biological weapons capability on equipment faces a similar problem

[16] For example, see Sammy Salama and Lydia Hansell, Does Intent equal Capability? Al-Qaeda and Weapons of Mass Destruction, *The Nonproliferation Review*, Vol.12, No.3, 2005, pp.615 - 653, p.639.
[17] Sammy Salama and Lydia Hansell, Does Intent equal Capability? Al-Qaeda and Weapons of Mass Destruction, *The Nonproliferation Review*, Vol.12, No.3, 2005, pp.615 - 653, p.639.
[18] Bob Graham et al., *World At Risk:The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, Vintage books, New York, p.35
[19] *Ibid.*, p.11.

to measures of chemical weapons capability. As Berkowitz notes, "[t]he equipment needed to make chemical and biological weapons (at least on a small scale) is virtually the same as the equipment used to make pesticides and brew beer)".[20] Attempting to measure capability based on knowledge also faces limitations given that this information is available via the internet, resulting in a potentially unknowable pool of people with knowledge of how to make basic biological weapons.[21] Additionally, due to the unpredictable advances in science and technology, future development and weaponisation a biological capability might not be identifiable.[22]

Similar to chemical weapons capability, successful biological weapons attacks have been used as a proxy-measure of capabilities of other non-state actors. The use of anthrax in letters posted in the United States in 2001, shortly after the 11 September attacks, is commonly referred to as evidence of the potential for non-state actors to develop biological weapons, and thus a proxy-measure of capability.[23] The attack killed five people, shut-down numerous postal and government offices, significantly slowed the postal system, and was successful in creating widespread public attention and fear. That it took the US Federal Bureau of Investigation nearly eight years to solve the case and name a principal suspect, illustrates the difficulty in identifying individuals involved in an attack, long after

[20] Bruce Berkowitz, Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, pp.289-300, p.292.
[21] For example, Howard and Sawyer observe that "for $28.50, any Internet surfer can purchase Bacteriological Warfare: A Major Threat to North America, which shows how to grow deadly bacteria that could be used in a weapon of mass destruction." Howard, Russell and Sawyer, Reid, *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004, p.xv.
[22] Coral Bell, *A World Out Of Balance: American Ascendancy and International Politics in the 21st Century*, Longueville Books, Double Day, 2003, pp.175-176.
[23] For example see, Elke Krahmann, From State to Non-State Actors: The Emergence of Security Governance, Elke Krahmann, *New Threats and New Actors in International Security*, Palgrave MacMillan, New York, 2005, p.4.

the event has occurred.[24] The use of the state's mail system to deliver the anthrax shows the difficulty of another proxy-measure of capability: a means of delivering the weapon. Unambiguous measure of a non-state actor's biological weapons capability might be the weapon, or more specifically the biological material itself. Again, it appears that confirmation of capability might only come from direct access to the individual or group and their resources.

There have been a number of attempted attacks using radiological weapons, or 'dirty bombs', which are seen as being within reach of many non-state actors. Nevertheless, radiological weapons are not on the same scale as the detonation of a nuclear device. A radiological device would be unlikely to kill large numbers of people, but rather the concern is related to the radiological contamination of a small geographic area and the potential for public panic.[25] Consequently, there have been debates over whether radiological weapons should be considered a weapon of mass *disruption* instead of a weapon of mass destruction.[26] Radiological weapons are included under the WMD section simply because they continue to appear under the title of WMD within intelligence and security agencies' own publications.[27]

The measures of a radiological weapons capability appear to rest upon radiological

[24] Refer to FBI website, available at: http://www.fbi.gov/anthrax/amerithraxlinks.htm accessed on 10 July 2009. The FBI alleges that the anthrax came from a US military establishment (United States Army Medical Research Institute for infectious diseases), indicating the fine line between state-development of materiel and their use by non-state actors (who was also a government employee). See: http://www.usdoj.gov/opa/pr/2008/August/08-opa-697.html.

[25] Henry Kelly, *Testimony to the Senate Committee on Foreign Relations, 6 March 2002*, available at: http://www.fas.org/ssp/docs/kelly_testimony_030602.pdf accessed on 5 July 2009.

[26] United States Nuclear Regulatory Authority, *Fact Sheet: Dirty Bombs*, March 2003 at: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs-bg.html

[27] For example, see United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, also Federal Bureau of Investigation definition of WMD: http://www.fbi.gov/hq/nsb/wmd/wmd_definition.htm accessed on 10 July 2009.

material, access to this material and access to explosives as a means of dispersal. In his testimony to the Select Committee on Intelligence of the United States Senate, the then Director of the FBI, Robert Mueller, raised concerns over the potential employment of dirty bombs due to the availability of small amounts of radioactive material on the open market and the minimal expertise required to develop such a device.[28] The International Atomic Energy Agency (IAEA) has recorded over 1,300 "…incidents of smuggling, theft, loss, illegal disposal and possession, and sales or attempted sales of nuclear or radioactive materials…" since 1993.[29] Radioactive materials that could be used in an attack are available at thousands of facilities (involved in medical and commercial research) in the United States alone, with varying levels of security.[30] The use of radiological devices has also been taken as a proxy-measure of the potential for other non-state actors developing and employing a radiological weapons capability. The most commonly referred to in this respect is the use of devices reportedly by Chechen separatists in 1995 and 1998.[31]

The ambiguity surrounding measures and proxy-measures of the development or acquisition of a radiological weapons capability leads to a similar conclusion as that for chemical and biological weapons capability. That is, confirmation of a radiological weapons capability appears to rely on direct access to the group and their resources. This is borne out by the United Kingdom's example of the arrest of two groups in 2004 on

[28] Robert Mueller, *Testimony of Robert S. Mueller, III, Director, FBI, Before the Select Committee on Intelligence of the United States Senate February 11, 2003*, available at: http://www.fbi.gov/congress/congress03/mueller021103.htm accessed 10 July 2009.
[29] International Atomic Energy Agency report http://www-ns.iaea.org/security/itdb.htm, accessed on 3 July 2009, referred to in United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, p.128.
[30] Henry Kelly, Testimony to the Senate Committee on Foreign Relations, 6 March 2002, available at: http://www.fas.org/ssp/docs/kelly_testimony_030602.pdf accessed on 5 July 2009.
[31] Details of these incidents are provided at: http://www.pbs.org/wgbh/nova/dirtybomb/chrono.html accessed 10 July 2009.

suspicion of undertaking planning for an attack using a dirty bomb.[32] What is evident is that the security agencies already had direct access to the group in order to make this assessment, and subsequent arrest. Unfortunately, as evident in the Russian experience, this access is not necessarily a given, making attempts to identify a radiological weapons capability a continuing difficulty.

Conventional weaponry appears to be an important measure for assessing capability, whether one is looking at state or non-state actors, although the types of weapons analysed differ. Unlike measures of state-based military weapons, which focus on large weaponry[33], non-state actors have used small arms and hand-held weapons. The 2008 Mumbai attacks were conducted by just ten individuals armed only with hand-held, conventional weaponry (machine guns, hand grenades, bombs), and yet killed 174 people.[34]

In contrast to the large, and expensive, military weaponry that can be imaged by satellite technology, the ubiquity and global proliferation of small arms limits the utility of small arms as a measure of capability. Estimates of the total number of small arms put the number at 640 million globally, with around two-thirds of these weapons held by people not in states' armed forces.[35] Reportedly, small arms are the principal cause of the death

[32] Jacqui Smith, '*Our shared values - a shared responsibility'*, First International Conference on Radicalisation and Political Violence in January 2008, available at: http://press.homeoffice.gov.uk/Speeches/sp-hs-terrorism-keynote-jan-08 accessed on 3 July 2009, referred to in United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, pp.29-30.

[33] For example, refer to National Intelligence Council, *Iraqi Military Capabilities Through 2003*, NIE 94-19, July 1994, Declassified, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.

[34] BBC, *Mumbai Attacks*, available at: http://news.bbc.co.uk/2/hi/in_depth/south_asia/2008/mumbai_attacks/default.stm, accessed 28 June 2010.

[35] See http://www.smallarmssurvey.org/files/portal/issueareas/inventories/inventories.html accessed 1 July 2009.

for over half a million people each year (in both wars and murders) around the world.[36] The global proliferation of small arms makes delineation between those non-state actors with or without these weapons difficult. In addition, the existing weapon stockpiles of specific non-state actors are not necessarily an accurate measure of their future small arms capabilities. Brian Jackson *et al.* highlight the example of the Provisional Irish Republican Army (PIRA), which learnt to manufacture bombs, mortars and RPGs immediately before an attack.[37] Consequently, "…estimates of stored weapons became a much less valid indicator of the group's capabilities and intent".[38] Thus, current weapons inventories, if confirmable, may not provide an accurate measure of a group's capabilities.

Non-state actors' access to secure more sophisticated military weaponry for conducting a mass-casualty attack has also increased in recent history, with man-portable air defence systems (MANPADS) being just one example. MANPADS are shoulder-launched missiles originally designed for use by state militaries to destroy aircraft and are able to be operated by just one person. These weapons have already been used both in successful and unsuccessful attempts to shoot down civilian airliners. In November 2002, there was an unsuccessful attempt to bring down a Boeing 757 Israeli airliner flying out of Mombassa airport in Kenya. In the attack, subsequently attributed to Al Qa'ida, two surface-to-air missiles were fired at the aircraft, but missed. Prior to this, in October 1998 a surface-to-air missile was reportedly used by Tutsi rebels in the Democratic Republic of Congo to successfully shoot down a Congo Airlines Boeing 727, resulting in the deaths of 41

[36] Elke Krahmann, From State to Non-State Actors: The Emergence of Security Governance, ed. Elke Krahmann, *New Threats and New Actors in International Security*, Palgrave MacMillan, New York, 2005, p.5.
[37] Brian Jackson et al., *Aptitude for Destruction Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, RAND Corporation, Santa Monica, 2005, p.50.
[38] *Ibid.*, p.50.

people.[39] Estimates place the number of MANPADS globally at 100,000, with most held by state militaries.[40] Nonetheless, despite attempts to prevent proliferation, these weapons have been described as "…cheap, widely proliferated, easy to use and conceal, and potentially lethal to all classes of aircraft".[41] In terms of MANPADS as a measure of capability, the potential limits on operability are underscored by Thomas Hunter, who argues that often confirmation that a non-state actor has access to MANPADS occurs with an attack itself.[42]

An argument can be made that the central measure of capability is people. Irrespective of whether one is assessing state-based or non-state threats, without people there is no capability. Thus, of all the measures, the measure of people is critical to any accurate assessment of capability. *Jane's World Armies* identifies a number of measures when arriving at the conclusions about the combat capabilities of armies. These factors include: the morale, professionalism and training of soldiers; overall numbers of full-time and reserve soldiers; command and control; and recent and current operations.[43] In reaching assessments about state's armies, much of this information is available via public sources, including government's own publications. As an example, when assessing the current morale of British army soldiers, *Jane's* uses the military's published reports to reach conclusions about the army's capabilities.[44] For non-state actors, similar measures might be applied, though accurate information might not be so readily available. Certainly, the

[39] Christopher Bolkcom, Andrew Feickert, Bartholomew Elias, *Homeland Security: Protecting Airliners from Terrorist Missiles*, Congressional Research Service, The Library of Congress, October 22, 2004, p.11
[40] James Bevan, Big Issue, Big Problem: MANPADS, *Small Arms Survey 2004: Rights at Risk*, accessed at: http://www.smallarmssurvey.org/files/sas/publications/yearb2004.html on 2 July 2009.
[41] Christopher Bolkcom, Bart Elias, Andrew Feickert, *MANPADs Threat to Commercial Aviation*, accessed at: http://www.ifri.org/files/CFE/CFEbolkcom.pdf on 1 July 2009.
[42] Thomas Hunter, The proliferation of MANPADS, *Jane's Intelligence Review*, 28 November 2002.
[43] Jane's World Armies, available by subscription http://jwar.janes.com, accessed 24 May 2010.
[44] *Ibid*.

covert nature of many of these groups makes determining morale, professionalism and training difficult. Command and control of non-state threats can be open to debate between experts, whilst linking people to recent and current operations may be achievable only years after the fact.

Taking estimates of numbers of people, it is apparent that applying this measure to state militaries is different, and often less difficult, than applying this as a measure of non-state actors' capabilities. As evident in *Janes' World Armies*, information on the total number of soldiers in state militaries is often publicly available, assisting analysts' efforts to assess states' military capabilities.[45] This is not necessarily the case with non-state actors, where the total number of people that make up a group or network is often difficult to define. As an example, Louis Freeh, then Director of the Federal Bureau of Investigation, estimated Al Qa'ida's numbers at the time to be between 10-25,000 veterans.[46] The inability to accurately identify the total numbers of people who make up Al Qa'ida potentially undermines the use of people as a measure a non-state actors' capability. Whilst governments compare the size of their own forces against other states' militaries to assess relative capabilities, a similar comparison is not necessarily possible for non-state capabilities. Despite lengthy conflicts with insurgencies in Iraq and Afghanistan, the actual numbers of insurgents have proven to be difficult, if not impossible, to assess. The argument that many of these are only part-time threat actors drawn into conflict inadvertently also hampers measures of people as a capability.[47] Indeed, a direct comparison potentially misses the true capability of non-state actors. The attacks of 11

[45] *Ibid.*
[46] Louis J. Freeh, Former Director, Federal Bureau of Investigation, testimony to *The Joint Inquiry on Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 08 October 2002.
[47] For a detailed discussion on this argument see David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Scribe, Melbourne, 2009.

September 2001 illustrate that non-state actors do not require thousands or even hundreds of people to affect a mass-casualty attack (even when the victims number in the thousands).

Increasingly, even when assessing state-based capabilities, assessments of people have devolved to the individual soldier as a measure of capability.[48] Jonathan Baily situates the soldier at the centre of military capability, noting that "…a well-trained and motivated soldier is the key to any military capability".[49] This measure of the individual capabilities of a soldier resonates in assessments of the threat posed by individuals within non-state groups. Bell argues that "[t]he ultimate asymmetric weapon is the suicide bomber: almost impossible to prepare against, and consuming very few military resources".[50] In addition, McConnell argues that assessing *capability* in a post-Cold War context is difficult as capability can be "…a single human being in a given place".[51] The idea of the individual as a capability is put forward in *Jane's Intelligence Digest's* argument that Al-Qa'ida uses its own people as its primary weapons.[52] Ersel Aydinli and James Rosenau contend that the difficulties in addressing terrorism are magnified by the use of the suicide bomber as a weapon. In particular, they highlight the practical problem facing intelligence and security agencies who "…cannot reach each and every possibility of suicide bombing by individuals who otherwise look normal and above suspicion".[53] The often covert

[48] For example, see Charles Krulak, The Strategic Corporal: Leadership in the Three Block War, *Marines Magazine*, January 1999.
[49] Jonathan Bailey, Strategy and Campaigning: End, Ways and Means, in Scott Hopkins (Ed.), *Asymmetry and Complexity: Selected Papers from the 2005 Rowell Seminar and the 2005 Chief of Army's Conference*, Land Warfare Studies Centre, Canberra, February 2007, pp.51-73, pp.71-72.
[50] Coral Bell, *A World Out Of Balance: American Ascendancy and International Politics in the 21st Century*, Longueville Books, Double Day, 2003, p.170.
[51] Mike McConnell, Director of National Intelligence (DNI), testimony to the Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007.
[52] Jane's Intelligence Digest, *More attacks - or paranoia?*, October 2001, accessed 10 January 2005.
[53] Ersel Aydinli and James Rosenau (Eds.), *Globilization, Security and the Nation-State: Paradigms in*

nature of threatening non-state actors hinders the use of people as a measure of capability.

One of the most consistently identified proxy-measures employed by analysts for assessing the threat of mass-casualty attacks is technology.[54] Indeed, Angus Muir makes the argument that "…the most obvious and important process in the 'modern age of terror …has been the development of technology itself".[55] There are three aspects that appear to influence the perception of *technology* as a proxy-measure of capability. These are:

1. Technological development and advances outside state-control;
2. Increasingly global access to and spread of tool, techniques and ideas; and
3. Adaptation of existing and new technology for mass-casualty attacks.

Increasingly, technological innovation, at one time led by the public sector, has shifted to the private sector, resulting in a global spread of technological expertise.[56] This makes consideration of potential capabilities a challenging proposition. Attempting to develop assessments of the potential capabilities that new technologies present is difficult. However, it is not simply 'new' technologies that have been employed to undertake mass-casualty attacks, but also adaptations (at times innovative) of *existing* technologies. As was evident with the September 11 attacks, the terrorist methods were ones of a low-technology approach. The technologies involved in that attack had been around for decades, but they

---

Transition, State University of New York Press, Albany, 2005, p.58.
[54] In this context, technology is defined as tools, techniques and knowledge.
[55] Angus Muir, Trends in the Development of Terrorist Bombing, in David Jones (Ed.), *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004, p.80.
[56] Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.56.

just had not been successfully employed in that manner before.[57] Thus, attempting to assess the innumerable potentially threatening uses of existing, new or emerging technologies appears impossible, given the sheer scale of tools, techniques and knowledge being developed and adapted. If, as it has been argued by the Department of Homeland Security, non-state actors can "…transform objects of daily life into weapons…"[58] then the benign nature of these objects limits the observability of technology as a proxy-measure of capability. Additionally, low-technology killing power is very difficult to counter. Max Boot highlights this in stating that "…when you think about the United States military, with a budget of over $500 billion and the most sophisticated technology on the planet, you would think that we would be able to defeat a simple device like the IED, and yet we have not".[59] It is little wonder, then, that Martin van Creveld labelled the era as "the invention of invention".[60]

The adaptation of already existing benign technologies or materiel into threatening forms is evident in the consistent and effective use of improvised explosive devices (IEDs) in Iraq and Afghanistan to conduct attacks against both military personnel and civilians. As Muir observes, the ubiquitous nature of bomb componentry, and the limited amount required for success, mitigate against usefully limiting supply.[61] This is evident from the 2005 London attacks, in which the bombers used commercially available substances to make the

[57] Edward Tenner, The Shock of the Old, in David Clarke (Ed.), *Technology and Terrorism*, Transaction Publishers, New Brunswick, 2004, p.8.
[58] Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.11.
[59] Max Boot, What are the Trends in International Security over the Next 20 Years?, *Australian Defence Force Journal*, No. 173, 2007, pp.13-24, p.20.
[60] Martin Van Creveld, *Technology and War: From 2000 B.C. to the Present*, Brassey's, London, 1991, pp.217-232.
[61] Angus Muir, Trends in the Development of Terrorist Bombing, in David Jones (Ed.), *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004, pp.86-87.

explosives,[62] with none of the purchases of the substances likely to have aroused suspicion.[63] In terms of observables for these material or technology required to develop bombs, there is a significant challenge in tracking, monitoring and, therefore, accurately assessing access to such elements.[64]

The use of technology to maximise awareness of an attack also increases the impact of a mass-casualty attack. This point is made by Bruce Hoffman, who observes that "the weapons of modern terrorism critically are not only the guns and bombs that they have long been, but the mini-cam, videotape, television, and the Internet".[65] The effects of a mass-casualty attack can achieve a strategic impact simply with the aid of cameras and global distribution of the images.[66] An extension could be seen as the idea of the "propaganda of the deed", in which the conduct of an attack is useful in gaining attention to garnering a following or encourage others to similar actions.[67]

Ownership of technologies is not necessarily an accurate proxy-measure of capability. As

[62] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, The Stationery Office, London, 2006, p.23.
[63] According to Quiggin, the bombers are reported to have used TATP (triacetone triperoxide), noting that "[t]he base ingredients for TATP are available in most states and can be bought as drain cleaner, bleach and acetone. All of these substances can be bought without raising suspicion from even a vigilant observer". Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific, Singapore, 2007, p.40.
[64] In the United States nearly five million tonnes of ammonium nitrate fertiliser, a key explosive component, are sold without any regulations. Brynjar Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions*, Routledge, London, 2005, p.185.
[65] Bruce Hoffman, *Inside Terrorism*, Columbia University Press, New York, 1998.
[66] Bruce Hoffman, Rethinking Terrorism and Counterterrorism Since 9/11, *Studies in Conflict and Terrorism*. Vol.25, 2002, pp.303-316, p.307. Thornton makes a similar observation, noting that "…small organizations, including Islamist ones, intent on causing severe damage to Western interests have only to look to the capabilities of a laptop, a modem, and some fairly common hacking skills to realize considerable effect". Rod Thornton, *Asymmetric Warfare: Threat and Response in the Twenty-First Century*, Polity Press, Cambridge, 2007, p.14. This at present is more financial and mass-disruption but not mass casualty, but as technology develops it might not be limited to just disruption.
[67] The idea of "propaganda of the deed" (or proganda by the deed) originated with 19th century anarchists. For a discussion of propaganda of the deed in modern attacks, refer to: Neville Bolt, David Betz & Jaz Azari, *Propaganda of the Deed 2008: Understanding the Phenomenon*, RUSI, Whitehall Report 3-08, 2008; and Alex Schmid, Terrorism as Psychological Warfare, *Democracy and Security*, Vol.1, No.2, 2005, pp.137-146.

non-state actors have demonstrated, they might simply borrow these from the society that they later attack. Andrew Smith defines capability as "…the degree of destruction of which the group is capable as determined by either the resources available or the destructive means possessed".[68] The issue of available resources is insightful, as a state's capabilities can be used against itself to devastating effect. On 11 September 2001 Al Qa'ida did not develop, or own, the technology or aircraft required to launch air attacks against US cities. Instead, they employed US civilian airliners, and knowledge and training gained from US flight training schools, against the US, and did so from within the country.[69] Consequently, looking for the group's physical resources, technologies or weapons that the 9/11 attackers would not have revealed any capability. Other benign technologies outside societies also appear to have been accessed to assist mass-casualty attacks. Following the November 2008 Mumbai attacks, a lawsuit was launched in India against Google claiming that the individuals involved in the attack had used satellite imagery from *Google Earth* to assist in planning the attacks.[70] Satellite reconnaissance imagery, once previously limited to states and their intelligence agencies, is now available to anyone with a computer and internet access.[71] The absence of assets required to commit an attack does not necessarily indicate an absence of killing-power. This more fluid idea of *access to*, rather than *ownership of*, raises the question of "whose technology needs to be assessed?". The assessment therefore broadens beyond the technologies and tools a non-state actor owns, to what a non-state

[68] Andrew Smith, Detecting Terrorist Activity: Defining the State's 'Threshold of Pain', *Australian Defence Force Journal*, No.168, 2005, p.35.
[69] The terrorists employed US civilian airliners that were flown by terrorists trained to fly in US flight training schools, money was funnelled through US banks, and they used US based communications.
[70] Refer to: Rahul Bedi, Mumbai attacks: Indian suit against Google Earth over image use by terrorists, The Telegraph, 9 December 2008, accessed on 28 June 2010 at:
http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html
[71] This observation is made by Boot who refers to reports that satellite imagery from Google Earth was used by insurgents in Iraq to assist in planning anti-Coalition attacks. Max Boot, What are the Trends in International Security over the Next 20 Years?, *Australian Defence Force Journal*, No.173, 2007, pp.13-24, p.17.

actor can access. The latter is a far broader and far more complex analytical challenge.

Cold War intelligence assessments looked at a state's economic potential for war-making as a proxy-measure of that state's capability to wage war.[72] Similarly, access to funds can be employed as a proxy-measure for assessing non-state capability. However, the relative costs of preparing and conducting a mass-casualty attack are on a far smaller scale than funding a war. Recent research has often focused on the relatively small cost of actually conducting an attack, particularly given the human and financial costs that such attacks can achieve.[73] A frequently quoted estimate of the direct costs of major mass-casualty attacks is from a 2004 report by the United Nations Monitoring Team on concerning Al Qa'ida and the Taliban. The report provided estimates of major mass-casualty attacks in the tens and hundreds of thousands of dollars.[74] Scott Atran estimates the material costs of mounting a suicide attack in Israel as low as US$150.[75] These estimates reinforce Rod Thornton's observation that costs involved in terrorist attacks "are certainly not prohibitive".[76]

There is, however, more to the cost of an attack than simply staging the attack itself.[77]

---

[72] National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950, accessed 31 October 2007 at: www.fas.org/irp/offdocs/nsc-hst/nsc-68-1.htm

[73] For example, see BBC, *London bombs cost just hundreds*, at: http://news.bbc.co.uk/2/hi/uk_news/4576346.stm accessed on 9 July 2009.

[74] United Nations, *First report of the Analytical Support and Sanctions Monitoring Team appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities, S/2004/679*, 25 August 2004 available at: http://www.un.org/Docs/journal/asp/ws.asp?m=S/2004/679 accessed on 9 July 2009.

[75] Scott Atran, The Genesis of Suicide Bombing, *Science*, Vol.299, 7 March 2003, pp.1534-1539, p.1537.

[76] Rod Thornton, Asymmetric Warfare: Threat and Response in the Twenty-First Century, Polity Press, Cambridge, 2007, p.46.

[77] This point has been emphasised by Prober who argues for a "de-bunking" of the paradigm of inexpensive terrorism. Joshua Prober, *Accounting for Terror: Debunking the Paradigm of Inexpensive Terrorism*, The Washington Institute for Near East Policy, Policy Watch No.1041, November 2005, available at:http://www.apgml.org/frameworks/docs/7/Costs%20of%20TF_J%20Prober%20Dec05.pdf accessed on 2 July 2009.

Estimates of the costs of launching attacks need to also take into account the cost of establishing and maintaining networks and infrastructure in the months and weeks prior to an attack.[78] This perspective is supported by a report of the inter-governmental Financial Action Task Force into terrorist financing, which divided terrorist financing into two general areas: funding specific operations, and broader organisational costs.[79] Of these, the most significant drain on finances is recruitment, planning and procurement to maintain a network or cell before an attack.[80] Nevertheless, information on the financing of specific operations, as well as estimates of broader operational costs, can prove difficult to obtain. Richard Clarke, former United States National Coordinator for Counterterrorism, highlights this in testimony to the Joint Senate and Congressional Inquiry into the 11 September attacks. Clarke notes that the intelligence community was "…unable to tell us what it cost to be bin Laden, what it cost to be al-Qa'ida, how much was their annual operating budget within some parameters, where did the money come from, where did it stay when it wasn't being used, how was it transmitted".[81]

When money is required for specific operations, the ability to track this funding is not guaranteed. The *hawala* system used for transferring money does not generate the collectable data that intelligence agencies rely on, thus funds can remain invisible to traditional collection methods.[82] In terms of pre-incident proxy-measures, funding attacks

[78] Joshua Prober, *Accounting for Terror: Debunking the Paradigm of Inexpensive Terrorism*, The Washington Institute for Near East Policy, Policy Watch No.1041, November 2005, available at:http://www.apgml.org/frameworks/docs/7/Costs%20of%20TF_J%20Prober%20Dec05.pdf accessed on 2 July 2009.
[79] Financial Action Task Force, *Terrorist Financing*, 29 February 2009, available at: http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf accessed on 3 July 2009, p.7.
[80] *Ibid.*, p.8.
[81] Richard Clarke, testimony, 11 Jun 2002 to *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, quoted in Joint Inquiry Final Report, p.117.
[82] Arthur Hulnick, Indications and Warning for Homeland Security: Seeking a New Paradigm, *International Journal of Intelligence and CounterIntelligence*, Vol.18, 2005, pp.593–608, p.601. Hawala is a remittance system which enables the transfer of money without actually moving the money, resulting in the absence of a

might not be distinguishable from non-threatening activities, given that funding can come from both legitimate and illegitimate means. The money used to finance the 2005 London bombings appears to have come from credit cards, with the unfortunate conclusion that funds from legitimate lenders appear to have been used to finance the attacks.[83] This provides an indication of the limitation of tracking funds as a proxy-measure for estimates of capability. A non-state actor might only require regular employment, and a good credit rating, to access the funds to carry out mass murder.[84] Whilst financial factors might assist in identifying indicators of an attack[85], they are evidently not a given.

What is a network capable of? Can anyone, even members of the network itself, actually know until they have actually attempted an attack? Unfortunately, given the limitation of measures and proxy-measures for assessing non-state capabilities, confirmation of these capabilities might be the actual attack itself. Further, the difference between *capable* and *incapable* might not be discernable either within the group or by analysts outside. Contrary to the state's more "tangible capabilities", the capabilities of non-state actors appear to be less measurable and, consequently, less certain.[86] Indeed, Bell makes the argument that Osama bin Ladin's lack of military assets was an advantage and it made it difficult for intelligence agencies to target him.[87] Because of the absence of large, tangible capabilities, "…al-Qa'ida [*sic*], as a non-state actor, could dare anything because it has no fixed assets

---

paper trail. The system is based upon trust with transactions occuring through communications between members of the hawala network. Refer to Patrick Jost and Harjit Sandhu, *The hawala alternative remittance system and its role in money laundering*, January 2000, accessed on 2 March 2011 at: www.interpol.int/

[83] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, The Stationery Office, London, 2006, p.23.

[84] *Ibid.*, p.23.

[85] Financial Action Task Force, *Terrorist Financing*, 29 February 2009, available at: http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf accessed on 3 July 2009, p.33.

[86] Mikhail Alexseev, *Without Warning: Threat Assessment, Intelligence and Global Struggle*, Palgrave Macmillan, Houndmills, 1997, p.267.

[87] Coral Bell, *A World Out Of Balance: American Ascendancy and International Politics in the 21st Century*, Longueville Books, Double Day, 2003, p.169.

that can be held at risk".[88] Without these tangible assets, analysts are required to infer assessments of capability, potentially leading to incorrect judgements.

The measures and proxy-measures detailed in this chapter do not necessarily provide clarity in the accurate assessment of non-state capabilities. Non-state actors do not need to employ large-scale military equipment, traditionally associated with state capabilities, to project killing power. Even where non-state actors do employ conventional weaponry, the small and ubiquitous nature of these weapons makes it difficult to rely upon this measure for accurately assessing capability. The conclusion is that the observability of measures and proxy-measures of capability that Singer employed for assessing state capabilities do not necessarily transfer to non-state actors.

Non-state actors lack the neat lines and numbers that provide analysts with a degree of certainty when assessing state capabilities. This makes assessment of non-state capabilities less certain and measures and proxy-measures more open to interpretation. In the absence of tangible measures for assessing capability, analysts are required to *infer*, rather than measure, non-state capabilities. The lack of measures or proxy-measures does not, however, mean that these non-state actors lack power. Instead, non-state actors can present a qualitatively different type of killing power to those possessed and employed by state actors. This, in turn, limits the observability of measures and proxy-measures, and undermines confidence in assessments of non-state capabilities.

[88] Coral Bell, *The First War of the 21st Century: Asymmetric Hostilities and the Norms of Conflict*, SDSC Working Paper No.364, Canberra, December 2001, p.2.

3.3 Estimating the Intent to conduct a mass-casualty attack

There is an argument that for non-state threats, it is *intentions* rather than *capabilities* which are the more certain parameter to assess.[89] Having examined at some depth the proxy-measures of capability, and the limitations of these, a critical analysis of the *indicators* used to assess intentions (and the observability of these indicators) is warranted.

In critiquing the indicators analysts use to make assessments of intent, a useful delineation is provided by Frank Stech in *Political and Military Intention Estimation: A Taxonometric Analysis*. Stech draws upon David Khan's distinction between "physical intelligence" (resources, installations, weapons), and "verbal intelligence" (words) which reflect the *object* of intelligence rather than a means of collection.[90] Stech argues that there are two ways of defining indicators of state intentions: as physical objects of physical intelligence; or as mental objects of verbal intelligence.[91] The following examination of indicators for assessing threatening non-state intentions adopts Stech's approach, dividing indicators into either *physical* or *verbal*.

The argument that military capabilities are a reflection and indicator of states' intentions is common within the intelligence literature.[92] The argument that military capabilities are

[89] See Mike McConnell, Director of National Intelligence (DNI), testimony to the Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007; and Robert Mandel, On Estimating Post-Cold War Enemy Intentions, *Intelligence and National Security*, Vol.24, No.2, 2009, pp.194-215, p.200.
[90] David Khan, *Hitler's Spies: German Military Intelligence in World War II*, Macmillan, 1978 quoted in Frank Stech, *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of Naval Research, Department of Navy, Maryland, November 1979, pp.8-10.
[91] Frank Stech, *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of Naval Research, Department of Navy, Maryland, November 1979, p.10.
[92] For example, refer to Roberta Wohlstetter, *Pearl Harbour: Warning and Decision*, Stanford University Press, Stanford 1962, p.364; David Lonsdale, *The Nature of War In The Information Age: Clausewitzian Future*, Frank Cass, London, p.210; and Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 2004, University Press of America, Maryland, p.92.

also an indicator of non-state intentions has been adopted and applied to non-state actors.[93] However, as the discussion on measures and proxy-measures of capabilities emphasised, the difficulties in accurately assessing non-state actors' capabilities undermine the utility of military capabilities as an indicator of intentions. The unconventional use of technology and the ubiquity of small arms and bomb-making componentry make accurate assessments of non-state actors' military, or killing, capability extremely difficult. There does appear to be some differentiation between groups that are identified prior to an attack and groups identified only after an attack. Where groups have been identified before an attack, these physical objects which may be used to kill, have been used as indicators of the group's intentions. The example of the United Kingdom Security Service's Operation Crevice illustrates this point.

Operation Crevice was an investigation by the United Kingdom's Security Service that led to the successful prosecution of five men on charges of plotting a mass-casualty event.[94] One of the members of the group purchased 600kg of ammonium nitrate and stored it in a London self-storage facility. Once the Police had confirmed the type and size of the material, the ammonium nitrate was considered evidence of both an *intent* and *capability* to conduct a mass-casualty attack.[95] The successful prosecution of the group involved, before any actual development of the material into an actual bomb, supports this assessment of the materiel as an indicator of intent (albeit in conjunction with additional indicators). Therefore, where suspicious individuals and groups have been identified, materiel held or

[93] For example, see Sundri Khalsa, *Forecasting Terrorism: Indicators and Proven Analytic Techniques*, Scarecrow Press Inc., Maryland, 2004, p.11.
[94] The investigation into this group by the UK's Security Service is referred to as Operation CREVICE. Further information on Operation CREVICE is available at: http://www.mi5.gov.uk/output/terrorist-trial-convictions.html accessed 09 July 2009.
[95] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2009, p.10.

accessed by the individual and group is taken as an indication of intent. However, even where individuals or groups are identified as suspicious, confirmation of a capability to conduct a mass-casualty attack is not guaranteed.

In the case of the 21 July 2005 attempted bombings in London, one of the individuals later convicted in the attempted attacks had come to the attention of British police on three occasions before the attempted attacks.[96] Nevertheless, whilst deemed suspicious, the individual was not identified as having the intention to carry out a mass-casualty attack. In terms of *capabilities*, as an indicator of intent, neither material nor devices that would later be used in the attempted attacks were identified by intelligence or security agencies. Indeed, given that materiel used for the bombs was a mixture of hydrogen peroxide and flour, it is questionable whether or not identification of this materiel alone would have been an unambiguous indicator of intent.[97] What is evident is that reliance on capabilities as indicators of intentions have has mixed success.

The actions and behaviour of non-state actors are consistently identified as an indicator of intentions. The former Director of the US Defence Intelligence Agency (DIA), Rear Admiral Lowell Jacoby, identifies the importance of collecting and exploiting information on terrorists' pre-incident behaviour and activity as a means of identifying intentions.[98] Pre-attack indicators of intentions are, however, not necessarily easy to identify.[99] The

[96] This was reported in evidence given at the court trial, reported at: http://www.independent.co.uk/news/uk/crime/london-bomb-suspect-had-come-in-contact-with-police-three-times-432574.html accessed 9 July 2009.
[97] This mixture was reported during the court case, detailed at: http://itn.co.uk/3967b7a45c8a1847f5ba6d060069a0ec.html accessed 9 July 2009.
[98] Lowell Jacoby, Director, Defense Intelligence Agency, Joint Chiefs of Staff, written submission to *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, p.4.
[99] For a broader consideration of threat-detection through analysis of behaviour, see John Hollywood et al.,

difficulty of pre-attack indicators of intent is acknowledged by Smith, who argues that the activities of groups preparing mass-casualty attacks "…tend to be low profile and often difficult to link with hostile intentions".[100] Sundri Khalsa lists a number of actions and behaviours that indicate an intent to conduct an attack, including: travel; training; physical surveillance; and tests of security.[101] Whilst these indicators might provide insight into intentions, even if information about the occurrence of such actions is received, it is not evident that such actions are clearly distinguishable from non-threatening behaviour or actions. Additionally, suspicious behaviour can indicate other illegal activity, such as espionage, theft and vandalism, and is not necessarily an unambiguous indicator of a preparation for an attack. Consequently, information on actions and behaviours can support multiple hypothesis of both legal and illegal activity, and are not necessarily evidence of preparations for a mass-casualty attack.[102]

This is not to suggest that indicators of intentions to conduct mass-casualty attacks are not identifiable prior to an attack. In a number of cases, intelligence and police agencies have been able to collect enough evidence of intentions to achieve successful prosecutions of individuals without an attack having occurred.[103] Despite this, the fact that some groups have been convicted does not mean that indicators are straightforward to identify, collect

---

Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior, RAND Corporation, Santa Monica, 2004. Unlike much of the intelligence literature, Hollywood et al. do not define threat in terms of *intentions* or *capabilities*. The approach is one of "connecting the dots" to identify *threatening behaviour* in the context of less tangible and more elusive adversaries coupled with enormous amounts of collected information.

[100] Andrew Smith, Preparation, Crisis and Consequence: Combating the New Threat of Mass-Casualty Terrorism, *Australian Army Journal*, Vol.1, No.1, pp.47-57, p.51.

[101] Sundri Khalsa, *Forecasting Terrorism: Indicators and Proven Analytic Techniques*, Scarecrow Press Inc., Maryland, 2004, p.11.

[102] Pope and Jonsang discuss how evidence can support multiple theories in their paper Simon Pope, Audun Josang, *Analysis of Competing Hypotheses Using Subjective Logic*, Proceedings of the 10th International Command and Control Research and Technology Symposium, 2005.

[103] United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, pp.27-28.

and accurately analyse. Unless linked to other physical or verbal indicators, it is potentially difficult to identify suspicious behaviour and actions as indicators of intentions.

The use of both written and spoken words as indicators of states' intentions has also been applied to non-state actors. In a similar way that words of state leaders are used, statements by leaders of non-state actors have been taken as indicating their organisation's or network's intentions. For example, public statements by Osama bin Ladin and Al Zawahiwi have been taken as indicators of Al Qa'ida's current and future intentions. Of particular note, Osama bin Ladin's response to a question on acquiring chemical and nuclear weapons, that acquiring these weapons in the defence of Muslims is a "religious duty"[104], was taken as an indicator of the broader organisation's intent to develop a WMD capability.[105] One potential limitation on relying on leader's words as an indicator of a group's intention is that this assumes a level of cohesion within an organisation that potentially does not exist.[106] Indeed, disagreements with an organisation's direction, evident within JI, spelt out earlier, illustrate that a single organisation might not be united in its intentions, and individuals can act independently of the organisation's purposes.[107] There is a difficulty with assessing intent based solely on the communication of organisation as this might not reveal what is actually happening within the organisation and may not identify cells which are acting independently of the group.[108] Whilst indicators of a leader's intentions may be available through public declarations, the covert

[104] Osama Bin Ladin quoted at:
http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/edicts.html accessed 9 July 2009.
[105] Sammy Salama and Lydia Hansell, Does Intent equal Capability? Al-Qaeda and Weapons of Mass Destruction, *The Nonproliferation Review*, Vol.12, No.3, 2005, pp.615 - 653, p.618.
[106] See Robert Mandel, On Estimating Post-Cold War Enemy Intentions, *Intelligence and National Security*, Vol.24, No.2, 2009, pp.194-215, p.211.
[107] Sidney Jones, *The Changing Face of Terrorism in Indonesia: Weaker, More Diffuse, and Still a Threat*, Speech to the Australian Strategic Policy Institute, 15 September 2005 at:
http://www.crisisgroup.org/en/publication-type/speeches/2005/the-changing-face-of-terrorism-in-indonesia-weaker-more-diffuse-and-still-a-threat.aspx.
[108] Author's interview with Dr David Kilcullen, 17 November 2005.

nature that is usually associated with preparations for mass-casualty attacks makes indicators of specific intentions difficult to acquire.

In considering the use of *open source intelligence* (publicly available information), Laqeuer argues that overt intelligence usually "…cannot give… specifics about the intentions and plans of adversaries or potential adversaries".[109] The continued debate over signals intelligence versus human intelligence as a means of obtaining indicators of intentions supports Laqeuer's argument.[110] Despite the use of telephone and email intercepts in prosecution of terrorist groups, there remains an argument that human intelligence is more appropriate to signals intelligence for analysts to gain insight into a threat actor's intentions.[111] This view was evident in testimony by Richard Clarke over the 11 September 2001 attacks, when he observed that "[s]ometimes you get lucky on communications intercepts, and if you put the jigsaw puzzle together, sometimes you can see intentions, but it is not the same as having a successful human, high-level penetration".[112] This appears to assume that only by gaining direct access to an individual can analysts obtain accurate verbal indicators of intentions. Even so, spoken and written words are regularly relied upon in the conviction of groups involved in planning mass-casualty attacks indicates that technical intercepts of spoken and written words are used as the basis for judgments on intent.

---

[109] Walter Laqueur, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, 1993, p.23.
[110] For example, Lowenthal highlights both signals and human intelligence in identifying *intent*, noting that "[s]ignals intelligence may help reveal intentions, but this collection task may require espionage". Mark Lowenthal, *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006.
[111] The enormous amount of telephone and email intercepts discussed earlier may also indicate the difficulty in acquiring unambiguous indicators of intentions of groups clearly attempting to disguise the true nature of their activities.
[112] Richard Clarke, testimony, 11 Jun 2002 to The Joint Inquiry into *Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*.

During the trial of a number of individuals convicted on terrorism charges as part of Operation Pendennis in Australia, the perceived importance of spoken and written words as an indicator of intent was evident. The Australian Federal Police collected over 97,000 telephone calls, around 16,400 hours of recorded conversation, and 26 gigabytes of internet traffic.[113] In the case of Operation Crevice in the United Kingdom, the Crown Prosecution Service argued that "[t]he intentions of the group were evidenced by conversations between the conspirators gleaned from listening devices strategically placed by the police".[114] Nevertheless, collecting words which provide unambiguous indicators of specific intentions is increasingly difficult, given the public awareness of intelligence collection capabilities.[115] Consequently, obtaining indicators of intentions is potentially becoming more difficult, even where intelligence agencies have identified potentially threatening non-state actors.

Unambiguous indicators of non-state threatening intentions appear to be difficult to identify. The intangibility of intentions as an indicator of non-state threat is potentially reflective of the dynamic and changing nature of the groups (and ultimately people within these groups) that agencies are attempting to identify and assess. Sidney Jones highlights the dynamic nature of JI's objectives which, she argues, has been assumed by many to have remained static based on "…looking at the organisation at a particular time and place:

---

[113] Karen Kissane, Tip-off led to intense 16-month investigation, *The Age*, 17 September 2008, at: http://www.theage.com.au/national/tipoff-led-to-intense-16month-investigation-20080916-4hxp.html?page=-1 accessed 09 July 2009.

[114] The Counter-Terrorism Division of the Crown Prosecution Service (CPS), at: http://www.cps.gov.uk/publications/prosecution/ctd.html accessed 9 July 2009.

[115] The most frequently cited example of this is claim made in the 9/11 Commission Report that the leaking of a US intelligence collection capability resulted in a change of communications by Al Qa'ida. As a consequence, the Commission alleged that the National Security Agency found it much more difficult to intercept bin Ladin's communications. See National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004, p.127.

Singapore and Malaysia in 2001".[116] Jones argues that JI, and therefore its objectives, is much more dynamic than this, and has undergone a number of changes in the years since 2001. The idea that intentions are dynamic and subject to change[117], potentially rapid change, based on the influence of personalities within non-state organisations or actions by authorities against the network, highlights the possible limitations of assessments. This raises legitimate questions over intentions, which include: how significantly do individual and group intentions diverge?; how often do individual intentions change?; and how often do group intentions change? Such questions begin to identify the limitations of assessments based upon indicators of intentions.

The dynamic nature of non-state actors, as well as the challenge of non-networked but 'inspired' threats, may indicate that groups themselves are not certain of their own intentions. Johnston argues that analysts, although they may be experts in their field, might not be able to assess and adversary's intentions, as the adversary might not know these themselves.[118] In an observation on assessing state leaders' intentions, and applicable to non-state leaders, Robert Mandel's observation that analysts may be attempting to know state leaders better than these leaders know themselves, applies to assessments of non-state leaders' intentions. Mandel highlights the faulty assumption that "[b]elieving that enemies are absolutely certain about their intentions can dangerously reflect the assumption that these intentions are static".[119] If an individual is not in the best position to make a clear explanation of their own current or future behaviour, what chance does an analyst have in

[116] Sidney Jones, The changing nature of Jemaah Islamiyah, *Australian Journal of International Affairs*, Vol. 59, No. 2, June 2005, pp. 169–178, p.171.
[117] Robert Mandel, On Estimating Post-Cold War Enemy Intentions, *Intelligence and National Security*, Vol.24, No.2, 2009, pp.194-215, p.211.
[118] Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study*, Center for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2005, p.66
[119] Robert Mandel, On Estimating Post-Cold War Enemy Intentions, *Intelligence and National Security*, Vol.24, No.2, 2009, pp.194-215, p.211.

assessing an individual? This is further complicated by the fact that analysts may be entirely removed from the context, space and time occupied by the non-state actor they are attempting to assess. Finally, there also exists the possibility of leaders deliberately attempting to undertake strategic deception within their public statements in order to disguise their actual purposes and future actions.

The issue of indeterminacy in intelligence analysis is discussed by Noel Hendrickson who argues that even if analysts knew everything about an individual terrorist, it would still not be able to infer with certainty what that individual will do.[120] Similarly, Cynthia Grabo argues that "[n]othing involving human behaviour is absolutely certain before it occurs".[121] Such indeterminacy was evident in the 21 July 2005 attempted bombings in London. One of the five individuals carrying bombs did not attempt to detonate their device, and instead reportedly dumped it in a bin and walked away, presumably deciding not to participate in the attempted attacks.[122] While indicators might be used to assess intentions, what is beyond question is that such indicators are limited in revealing what is *actually* going to happen. Analysts are attempting to assess intentions for very small groups and individuals, meaning that ultimately indicators of intent must be tied back to an individual's inner thoughts. Unfortunately, such inner thoughts might not present analysts with many observable indicators of intent. Yet, as recent history indicates, an absence of observable indicators of intentions is not necessarily evidence of the absence of hostile intentions.[123]

---

[120] Noel Hendrickson, Critical Thinking in Intelligence Analysis, *International Journal of Intelligence and Counterintelligence*, Vol21, No.4, 2008, pp.679-693, p.681.
[121] Cynthia Grabo, *Anticipating Surprise: Analysis for Strategic Warning*, 2004, University Press of America, Maryland, p.20.
[122] BBC, *21 July: Attacks, escapes and arrests*, http://news.bbc.co.uk/2/hi/uk_news/6752991.stm accessed 5 July 2009.
[123] The Madrid bombings are an example in which no indication of an intent to conduct the attacks was identified prior to the attack. The successful conduct of the attack illustrates that intelligence agencies may not identify indicators of preparations for an attack, even though planning for the attack is occurring.

3.4 The Post-hoc Use of Capability and Intent

There is a tendency for analysts to base assessment of non-state actors' current or future intentions and capabilities on previous attacks. In this way, capability and intent are applied in a post-hoc manner, as evident in publicly released intelligence analysis. Assessments by ASIO over a two-year period illustrate this tendency to equate attacks with future intentions and capabilities. In their 2003-2004 Report to Parliament, ASIO assessed that "[t]errorist attacks in Indonesia, Spain, Turkey, Morocco, Saudi Arabia and some in Iraq over the past year underlined the continuing intent and capability of groups such as al-Qa'ida and Jemaah Islamiyah".[124] Previously, in its 2002-2003 report, ASIO assessed that "Al-Qa'ida retains the intent and capability to undertake acts of terrorism around the world, as demonstrated with attacks in Kenya in November 2002 and in Riyadh on 12 May 2003".[125] The US 2001 *Quadrennial Defence Review* provides an example of an attack by one group being taken as an indication of capabilities and intentions of groups more broadly, again a questionable assumption. The Quadrennial Defence Review states that "[t]he attacks against the US homeland in September 2001 demonstrate that terrorist groups possess both the motivations and capabilities to conduct devastating attacks on US territory, citizens, and infrastructure".[126] An alternate assessment might be that the 11 September 2001 attacks demonstrated that only Al Qa'ida could only conduct an attack of that scale, and no larger. Additionally, the attacks could be taken as evidence that *only* 19 members of Al Qa'ida were able to carry out such an attack and with their deaths no other members of the group had either the intentions or capabilities. Further, the lack of

[124] Australian Security Intelligence Organisation, *Report to Parliament 2003-2004*, Commonwealth of Australia, Canberrra, 2004, p.3.
[125] Australian Security Intelligence Organisation, *Report to Parliament 2002-2003*, Commonwealth of Australia, Canberrra, 2003, p.16.
[126] Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., September 2001, p.5.

additional attacks by Al Qa'ida immediately after September 2001 could be an indication that Al Qa'ida was only able to conduct the one coordinated attack within the US.

Where attacks are used as a post-hoc measure, or as an indicator of both current and future intentions and capabilities, the accuracy of such post-event assessments is questionable. In such cases, there appears to be an assumption that a group's capability is not only undiminished, but their intent is to immediately replicate the successful attack.[127] But such an assumption may be inaccurate. Instead, there is a strong argument to suggest that the capability of a group to replicate an attack is immediately diminished following a successful mass-casualty attack. One reason for such an approach is that where an attack utilises suicide as a tactic, the threat actor loses people. Another is that security is understandably tighter following such events. Thus, concerns over a repeat of, or similar scale attacks, 11 September 2001 proved incorrect, potentially because of both Al Qa'ida itself having spent its ability to launch such attacks for the time being, as well as the US having increased security measures and undertaken military action in Afghanistan. As a consequence, an argument could be made that Al Qa'ida's capabilities, and even their intentions, to conduct mass-casualty attacks were actually diminished following 11 September 2001.

The assumption that a group's aims or abilities are clear once an attack has occurred is questionable. For example, John Baker argues that the 2004 attack on the Australian Embassy in Jakarta, Indonesia "demonstrated JI's continuing capabilities for executing

[127] Kie Fallis notes "an inexplicable tendency" for some intelligence agencies "…to issue warning reports and raise the terrorism threat level after an attack". Kie Fallis, Statement for the Record: Lessons Learned and Actions Taken in Past Events, 8 October 2001, written submission to *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, p.7 at: http://www.fas.org/irp/congress/2002_hr/100802fallis.pdf.

major bombing attacks".[128] However, Baker also highlights the lack of clarity when considering the purpose of the attack, noting that "if the operational and political intent of the attack was to inflict substantial casualties on Australian embassy personnel, particularly foreigners, it fell quite short of the desired result".[129] Whilst the desire (intent) to conduct the attack was evident from the attack itself, if the purpose (intent) of conducting the attack remains uncertain, then assessments of the likelihood of future attacks appear limited. If analysts are unable to determine 'why' an attack occurred, how are they to make accurate or insightful assessments of the potential for future attacks? Indeed, applying the parameters of threat post-hoc may lead analysts to incorrect conclusions about non-state threats, particularly when many details of the attack might only become evident years after the event, or perhaps not at all.[130]

[128] John Baker, Jemaah Islamiyah, in Brian Jackson et al (Eds.), *Aptitude for Destruction Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, RAND Corporation, Santa Monica, 2005, p.71.
[129] *Ibid.*, p.71.
[130] The release of the London Bombing report some four years after the actual event is indicative of the delay and difficulty in obtaining information about an event even once it has happened.

Chapter 4

A Critique of Singer's Model as Applied to Non-State Actors: Towards a More Comprehensive Concept of Threat

> The traditional measure of threat—capability plus intent equals threat—applied to today's global security environment is an elusive equation.
>
> Melissa Applegate [1]

4.1 Critiques of Singer's Model

The model of threat described by Singer has been near-universally adopted and applied within the intelligence analysis literature for assessing both state-based and non-state threats. Despite this widespread acceptance of the dominant episteme, there have actually been few deliberate critiques of the conventional model. Instead, as noted in Chapter 3, much of the debate over threat assessment has occurred within the parameters of Singer's model. Consequently, there are only a small number of authors who have deliberately considered the foundational concept of threat rather than uncritically adopting the model.

As noted in Chapter 1, in his paper *Intelligence Methodologies Applicable to the Madrid Train Bombings,* Glen Segell argues that the trends and patterns approach, which "…can be equated with and referred to as the analysis of intent and capability", remains the most significant methodology for state-based conflict, diplomatic intelligence, the primary methodology for military intelligence analysis.[2] Segell goes beyond describing the

[1] Melissa Applegate, *Preparing for Asymmetry: As seen through the lens of Joint Vision 2020*, Strategic Studies Institute, Carlisle Barracks, September 2001, p.8.
[2] Glen Segell, Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004, *International*

approach to a deliberate critique, highlighting examples where such a methodology has proven inadequate in providing insight into significant events below a state-level of analysis. The French Revolution (1789), Sepoy Revolt (1856) in India, the numerous coups and revolutions that followed decolonization, even the demise of the Soviet Union, are provided as examples where the conventional model has failed to identify threats ahead of the event. Segell's explanation for the failure of the methodology is that these were *substate* events and did not involve an identifiable build-up of capability by state forces, nor political hierarchies whose intentions could be observed.[3] The lack of measures or indicators cited by Segell echo the difficulties in assessing non-state threats.

Segell provides an additional, important insight into Singer's model of threat in presenting an argument as to why the dominant episteme has become ingrained in intelligence analysis. As noted previously, according to Segell, the continued reliance on this approach is based on its success and simplicity in training and coping with staff turnover in intelligence agencies.[4] The use of this method has enabled new staff to quickly focus on gathering data and conducting analysis using this well-established technique.[5] If the immediate training and indoctrination analysts receive involves a concept of intelligence as the *analysis of intent and capability*, and of threat as intent and capability, then it is little wonder that the model has largely avoided attracting deep and detailed critique. If this methodology for assessing threat is constantly reinforced throughout analysts' careers, and then, in turn, used and reinforced by these same analysts to train junior analysts, then it is apparent why such a concept simply becomes accepted. Consequently, changes in the

---

Journal of Intelligence and Counterintelligence, Vol.18, No.2, pp.221-238, p.224.
[3] *Ibid.*, p.227.
[4] *Ibid.*, pp.224-225.
[5] *Ibid.*, pp.224-225.

context of threat do not result in a corresponding questioning over the applicability of the conventional approach to assessing threat. Instead, concepts of threat remain based upon intent and capability not because of rigorous examinations of alternatives but because the traditional concept is the only one taught.

Despite the continuing dominance of this actor-based approach, a small number of researchers have questioned certain assumptions which underpin the model; at least where the focus is on assessing threats from states. In their analysis of decision-making, Cynthia Kurtz and David Snowden argue against the assumption of intentional capability in the analysis of state behaviour. Kurtz and Snowden argue that "intentional capability", whereby a state acts deliberately rather than accidentally, is an assumption that does not hold in all circumstances. Yet methodologies used in policy analysis and decision-making, such as the one described by Singer, assume that states only act deliberately.[6] Instead of assuming intentional capability, Kurtz and Snowden argue that the focus becomes one of considering the context of a state's action such that analysts ask: "What does it mean that this happened?" rather than "What did they have in mind when they did that?".[7] This freeing the link between intentions and capabilities is an interesting one, leading to the suggestion that factors external to actors, even state actors, might influence the decisions or outcomes that states choose or are forced to make.

In analysing US intelligence agencies' performance in anticipating the collapse of the Soviet Union, *Stratfor* provides a valuable critique of the conventional approach to threat assessment. *Stratfor* argues that US intelligence agencies' focus on capabilities and

[6] C. Kurtz and D. Snowden, The new dynamics of strategy: Sense-making in a complex and complicated world, *IBM Systems Journal*, Vol.42, No.3, 2003, p. 463.
[7] *Ibid.*, p.482

intentions, whilst it "…seems perfectly logical, it is almost designed to generate not so much the wrong answer as an irrelevant answer".[8] According to *Stratfor*, the CIA's fundamental error was the obsession with attempting to understand President Gorbachev's intentions. In the case of the Soviet Union, the argument is that Gorbachev's intentions were irrelevant; the collapse of the Soviet Union reflected global factors beyond the control of Gorbachev or any other member of the Soviet leadership, and certainly not a reflection of intent.[9] *Stratfor's* argument is that external factors, beyond deliberate control of hierarchies or leaders, influence a state's actions. As a result, the focus on intentions results in surprise, as behaviour is not simply a reflection of intent, but more so of external factors and unintended consequences.

Such perspectives notwithstanding, critiques of the Singer model itself remain the exception rather than the rule within. Nevertheless, and particularly since 11 September 2001, a number of different analytical approaches to assessing threat have gained popularity, even whilst critiques of the conventional model have been limited. The very existence of such alternative approaches highlights that the conventional model, whilst not necessarily the subject of much deliberate critique, does have practical limitations in addressing non-state threats.

4.2 Alternative Approaches for Assessing Threat

Despite the dominance of Singer's actor-based approach, alternative methodologies for

[8] Stratfor, *Focused on the Trees, the CIA Missed the Soviet Forest's Fall*, Mar 12, 2001, accessed at: http://www.stratfor.com/products/premium/read_article.php?id=101528 (by subscription) on 07 Mar 2006.
[9] *Ibid*.

threat assessment do exist.[10] At the most generic level these can be described as: a vulnerability approach; an environmental approach; and a situational approach. As will be discussed, the first two of approaches are already evident within intelligence and security debates, albeit without necessarily being consciously defined as alternatives to the conventional model. The third approach draws on social psychology research into how external factors may impact the behaviour of individuals. These alternative approaches will now be examined, with a brief consideration of their potential as alternative approaches as well as the potential of adding elements of each of these in addition to the conventional model in order to provide a more comprehensive approach to assessing threat.

4.2.1 Vulnerability Approach to Threat

One alternative to the actor-based approach, which gained increased attention in the aftermath of the 2001 Washington and New York attacks,[11] can be described as a vulnerability-approach to threat assessment. However, the identification of state vulnerabilities is not necessarily a new approach to assessing threat. As is evident within state-based threat assessments during the Cold War, analysis of a state's own vulnerabilities in relation to the perceived threat from another state did occur.[12] Within the context of non-state threats, this focus on the state's vulnerabilities has continued, albeit with a recognition that these vulnerabilities are not on the same scale as the vulnerability to nuclear warfare between states.[13] There is, however, a distinct difference between the use

[10] It is worth making a comment on the use of scenarios. Whilst it might be argued that scenarios could be considered an alternative approach to assessing threat, scenarios tend to be used to explore possible threatening *situations*, rather than for assessment of threats.
[11] Brian Jenkins, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica, 2006, p.151.
[12] For example, see National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950, accessed 31 October 2007 at: www.fas.org/irp/offdocs/nsc-hst/nsc-68-1.htm
[13] For example, the US National Strategy for Homeland Security argues that, in addition to knowing the

of vulnerability-approach where the threat is state-based compared with those where the threat is non-state based.

Where a state's vulnerabilities are assessed against those of another state, such an assessment is based upon knowledge of a clearly defined threat actor. By contrast, the increased use of a vulnerability-approach to assessing a state's vulnerabilities against non-state threats is due to the *absence* of a clearly defined threat. Brian Jenkins argues that it was precisely the difficulties in assessing intentions and capabilities of terrorist organisations which resulted in analysts adopting vulnerability-based assessments after the September 11 attacks. According to Jenkins, during the Cold War the assessment of the Soviet threat was easy, as intentions were manifest and assessments focussed on capabilities.[14] In contrast, terrorism presents a number of difficulties for analysts: terrorists are more difficult to understand; intelligence is more difficult to acquire; terrorist actions are difficult to predict; targets of terrorists are virtually unlimited.[15] These uncertainties caused a shift from threat-based assessments to vulnerability-based assessments.[16] In *The Shield of Achilles*, Philip Bobbitt, a notable proponent of a vulnerability-based approach, argues for a vulnerability approach to threat assessment, based on recognition of the potential ambiguity of the perpetrators of mass-casualty attacks. According to Bobbitt, thinking must shift from threat-based strategies (which rely on knowledge of threat actors) to vulnerability-based strategies.[17] Vulnerability is usually associated with the assessment of risk. For example, Henry Willis *et al.* use vulnerability as one of three parameters for

---

enemy, the more the US understands "…about our vulnerability, the better able we are to protect ourselves". Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002, p.7.

[14] Brian Jenkins, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica, 2006, p.151.

[15] *Ibid.*, p.151.

[16] *Ibid.*, p.151.

[17] Philip Bobbitt, *The Shield of Achilles*, Penguin Group, London, 2003, p.812-813

assessing terrorist risk, the other parameters being those of threat and consequence.[18] However, within the context described by Bobbitt and Jenkins, vulnerability appears to have become a parameter used for directly assessing threat in the absence of identification and knowledge of a specific threat actor.

Perhaps one of the most obvious applications of such a methodology is the discourse on "homeland security", on the strength of which the Government of the United States established an entire agency "…to secure our country against those who seek to disrupt the American way of life".[19] This priority of securing the homeland is a reflection of a vulnerability assessment, in which priority is given to the location where the greatest numbers of citizens live. Thus, one benefit of a vulnerability-methodology in assessing threat is that the referent (i.e. a state's citizenry) is clearly definable, even if the threat actor is not. Consequently, the approach shifts analysis from a difficult-to-identify threat actor to a less-difficult-to-identify *threatened* actor. Analysts are able to identify where large numbers of a state's citizens travel to and live, both within the state as well as internationally. Indeed, a change in the focus of assessment from the threat actor to the referent means that a vulnerability-approach to threat assessment can also be described as an actor-based approach. Instead of the focus on identifying a *threat actor* (based on *intent* and *capability*), a vulnerability-approach is similarly focused on identifying a different actor, the referent or those actors potentially threatened. Thus, we might define the conventional approach as a *threat-actor approach* and vulnerability as a *referent approach*.

[18] Of note, Willis *et al.* adopt Singer's dual-parameter concept of threat. Henry Willis, Andrew Morral, Terrence Kelly, Jamison Medby, *Estimating Terrorism Risk*, RAND, Santa Monica, 2005, pp.5-11. For an additional example of the use of vulnerability as a parameter in assessing the risk of an attack by a non-state actor, refer to Hank Prunkun, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Lanham, 2010, Chapter 11, pp.172-179.

[19] Department of Homeland Security, http://www.dhs.gov/xabout/strategicplan/ accessed on 21 November 2009.

One argument that could be raised against such an approach is that intelligence focuses on threats and not vulnerabilities. This can be equated with the argument that intelligence focuses on 'red' (an enemy or adversary) not 'blue' (the analysts' own state or friendly entity). However, even if one was to take the conventional model of intentions and capabilities, it is apparent that analysts using this approach are actually considering the threat to their own state or friendly entity. This is because that intentions and capabilities are assessed *in relation to* someone or something, regardless of whether or not this is assumed or not defined.

A vulnerability-approach, however, does appear to face similar limitations to the more dominant threat-actor approach. As discussed in Chapter 3, just as the numbers of non-state actors who *could* pose a mass-casualty threat is too great for any single intelligence agency to address, the potential numbers of vulnerabilities in any Western society "are essentially infinite".[20] Jenkins makes the point that, in a large industrial country, the potential targets for terrorist attack are "virtually unlimited" and highlights numerous possible targets based specifically solely on Al Qa'ida. According to Jenkins:

> A complete catalogue would include commercial aircraft and airports, subways and trains, cruise ships and ferries, cargo vessels and port facilities, bridges and tunnels, refineries and pipelines, power lines and transformers, nuclear power plants, reservoirs and waterworks, food-processing facilities, financial institutions, government buildings, foreign embassies, landmark properties, tourist sites, churches, synagogues, temples and mosques, hospitals, sports arenas, shopping malls, any place people gather. All of these meet the al Qaeda [*sic*] training manual's criteria for target selection: "sentimental value" or "high human" intensity. All have been targets of terrorists in the past. All vie for attention and

[20] Paul Davis and Brian Jenkins, *Deterrence and Influence in Counterterrorism: A Component in the War on Al Qa'ida*, RAND Corporation, Santa Monica, 2002, p.xiv.

resources today.[21]

Similarly, in *The Geometry of Terrorism*, Donald Black argues that technology, modern architecture and engineering collects and confines masses of people unable to defend themselves against threats whose perpetrators blend into these same crowds.[22] International travel also means that citizens are potentially placing themselves within reach of non-state actors, who would otherwise be unable to conduct mass-casualty attacks.[23] The referents of mass-casualty attacks are potentially now physically within the same geographic areas as threat actors, resulting in an increase in vulnerabilities.[24] Therefore, a vulnerability-approach appears to face similar limitations in terms of the overwhelming number of potentially *threatened-actors* down to the individual level. Further, if the approach only considered referents of threat without regards to potential threat actor, it would similarly fail to reflect the complexity inherent in the concept of threat. Nevertheless, as a fundamental part of the broader ontology of threat described in Chapter 2.1, the referent is a foundational entity that needs to be considered within any comprehensive approach to threat assessment. Thus, whilst a vulnerability-only approach to assessing threat would be similarly limited as a threat actor-only approach, the inclusion of vulnerability in terms of a referent does present an opportunity for a more *comprehensive* model of threat. Further, given that threats are assessed in relation to something, then any actor-based model would need to factor in possible vulnerabilities. Without defining or articulating a referent,

[21] Brian Jenkins, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica, 2006, pp.151-152.
[22] Donald Black, The Geometry of Terrorism, *Sociological Theory*, Vol.22, No.1, March 2004, pp.14-25, pp.23-24.
[23] The 2002 Bali bombings is one such example of large numbers of Australians and British citizens being killed outside their nation's borders. That both nations conducted formal reviews into the intelligence available prior to the attacks indicates an expectation that intelligence agencies have a responsibility to identify and warn of threats to citizens beyond the geographic confines of the state.
[24] Donald Black, The Geometry of Terrorism, *Sociological Theory*, Vol.22, No.1, March 2004, pp.14-25, pp.21-22.

attempts at assessing threats are partial at best. Thus, a more comprehensive approach to assessing threat requires the identification of a referent upon which assessments of threats (external to the referent) can commence.

4.2.2 Environmental Approach to Threat

The second alternative approach to be considered can be described as an environment approach to assessing threat. In this, threat actors and referents are conceptualised within a broader environment. For example, Melissa Applegate argues that "[t]he traditional measure of threat—capability plus intent equals threat—applied to today's global security environment is an elusive equation". [25] Applegate's observation indicates that there are limitations in applying the traditional concept to assessing non-state threats. Interestingly, Applegate nonetheless applies Singer's concept within the context of a *global security environment*. This application of the conventional model *within* a broader *environment* is not without precedent. Antulio Echevarria similarly argues that "[t]oday's threat environment reflects the influences of a faster-paced and more interconnected world. In this environment, the more traditional notion that 'a threat = capabilities x intentions' remains valid, but [that this equation] requires more emphasis on potential threats than previously".[26] Echavarria applies Singer's model within the concept of a broader, overarching security environment and draws conclusions over the applicability of the model within this context.

Bill Flynt undertakes a comparable approach in situating Singer's concept of threat within

[25] Melissa Applegate, *Preparing for Asymmetry: As seen through the lens of Joint Vision 2020*, Strategic Studies Institute, Carlisle Barracks, September 2001, p.8.
[26] Antulio J. Echevarria III, The Army and Homeland Security: A Strategic Perspective, Strategic Studies Institute, Carlisle Barracks, March 2001, p.6.

a *security environment*.[27] But Flynt goes further by developing a working concept of the security environment and defining the elements within it. According to his model of the security environment, there are three elements involved: *threat, environment* and *self*.[28] Within this concept, threat can be equated to the threat actor and self as the referent. Of these three elements, Flynt argues that, whilst understanding *self* and the *environment* has changed relatively little, it is the understanding of *threat* which has become more difficult. His conclusion on assessing threats is that the proliferation of military capabilities means that determining intent should be the key focus in identifying threats.[29] Such a conclusion situates Flynt's critique as a debate *between* the parameters (see Chapter 3). Nevertheless, he moves the debate beyond simply an analysis of *red* (threat) and *blue* (self) and includes these within, what he describes as, a broader *grey* space (environment). Flynt's idea of a *security environment* within which both threats and threatened exist is worth considering, particularly given the concept has gained such widespread usage and acceptance in recent years.[30] The concept of a *security* or *threat environment* is not new,[31] however the concept appears to have taken on an increased importance in efforts in grappling with the analytical

---

[27] Bill Flynt, Threat Kingdom, *Military Review*, July-August, 2000, pp.12-21, pp.12-13 & p.21.
[28] *Ibid.*, pp.12-21, p.13.
[29] *Ibid.*, pp.12-13 & p.21.
[30] This approach has both similarities and differences with the *Intelligence Preparation of the Battlefield* (IPB) approach employed within the US Armed Forces (refer to *FM 34-130 Intelligence Preparation of the Battlefield*). The IPB process is described as "…a systematic, continuous process of analysing the threat and environment in a specific geographic area". Whilst employing the concept of an environment, the context of the IPB is singularly military. The initial step within the IPB process is to define the *Battlefield environment*, with the battlefield principally defined within a military context. The battlespace consists of an *Area of Operations* (i.e. where military forces are physically deployed) and an *Area of Influence* (defined geographically as areas which – whether militarily or politically – have an influence on the battlefield, whether directly or indirectly). As a result, the area of operations is able to be clearly defined and, as a consequence, the focus of assessments of threat is 'contained' to a well-defined physical space. Medby and Glenn provided a useful critique of the IPB process in *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations*. It is worth highlighting that both the IPB process and Medby and Glenn's adaptation are still tied to Singer's model of threat, defining threats in terms of *intentions* and *capabilities.*
[31] For example, refer to Paul Dibb, *Review of Australia's Defence Capabilities*, Report to the Minister for Defence, March 1986, p.35 ("threat environment"); Ministry of Defence, *Strategic Defence Review*, The Stationery Office, London, July 1998, para 23 ("security environment"); National Security Council, *A National Security Strategy for a New Century*, White House, Washington, D.C., December 1999, p.5 ("international security environment").

and conceptual challenges presented by non-state threats. As evident below, within government, defence and intelligence publications, the employment of the concept of a threat environment is particularly apparent.

The United States' report *National Security Strategy*, released following the September 2001 attacks, highlights concerns over non-state actors, with a determination to obtain the destructive power previously limited to states as making "...today's *security environment* more complex and dangerous".[32] The Federal Bureau of Investigation's *Intelligence Philosophy* states that "[t]he tool of intelligence is more important than ever in today's *threat environment*".[33] The 2010 *Quadrennial Defence Review* argues that the Department of Defence be able to protect the nation and US allies in "this dynamic *threat environment*".[34] At Senate Committee hearings six years after the 11 September 2001 attacks, the Secretary of the Department of Homeland Security, the Director of National Intelligence, the Director of the FBI, and Director of the National Counter Terrorism Centre were specifically asked to provide an "…evaluation of the current *threat environment*".[35] The US military has developed an environmental approach to intelligence analysis in support of military operations. The Joint Intelligence Preparation of the Operating Environment (JIPOE) has been developed as a "macro-analytic approach" to assist in understanding an *operating environment*.[36]

---

[32] George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, p.13. Italics added by author.
[33] Federal Bureau of Investigation, *Intelligence Philosophy*, at: www.fbi.gov/intelligence/philio.htm accessed 13 October 2009. Italics added by author.
[34] Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 2010, p.32. Italics added by author.
[35] Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007. Italics added by author.
[36] The operating environment is defined as "…a composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander". Joint Chiefs of Staff, *Joint Intelligence Preparation of the Operational Environment*, Joint Publication 2-01.3, 16 June 2009. Italics added by author. Interestingly, JIPOE still rests on Singer's model. The Joint Chiefs of Staff

The concept of an environment is evident within Australian Government publications, which also captures the idea that individual actions are able to influence, even shape, this environment. In Australia, the Department of Prime Minister and Cabinet's publication *Protecting Australia Against Terrorism* argued that both the 11 September 2001 and the 2002 Bali attacks indicated a "new *security environment*".[37] According to this publication, a single event, the September 2001 attacks, "changed the global *strategic environment*".[38] Within this context, the then head of the Prime Minister and Cabinet (PM&C), Andrew Metcalf, in a speech titled *Australia's National Security Preparedness*, spoke of the Government's preparation to "…meet the challenges of the new *threat environment*".[39] Then Minister of Defence, Robert Hill, argued that "[t]he single theme that characterises the *security environment* that we will experience over the next decades is uncertainty".[40] The *2007 Defence Update* argues that globalisation is "reshaping our *security environment*".[41] More recently, the former Prime Minister Kevin Rudd released Australia's *National Security Statement*. Amongst the ideas captured in this document is the concept of a current and future "*security environment*" characterized by fluidity, complexity and dynamism.[42] According to the Department of the Prime Minister and Cabinet's 2010

---

publication notes that "[t]he JIPOE process - defining the operational environment, describing the impact of the operational environment, evaluating the adversary, and determining adversary COAs [courses of action] - provides a disciplined methodology for applying a holistic view of the operational environment to the analysis of adversary capability and intent". *Ibid.*, p.xvi.

[37] The Department of Prime Minister and Cabinet, *Protecting Australia Against Terrorism*, Commonwealth of Australia, Canberra, 2004, p.vii. Italics added by author.

[38] *Ibid.*, p.2. Italics added by author.

[39] Andrew Metcalf, *Australia's National Security Preparedness - Where Next?*, presentation to Security in Government Conference 2005, Attorney-General's Department. Italics added by author.

[40] Robert Hill, *The Changing Security Environment*, Speech, 24 January 2004. Italics added by author.

[41] Department of Defence, *Australia's National Security: Defence Update 2007*, Commonwealth of Australia, Canberra, p.14. Italics added by author.

[42] Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008. Italics added by author.

Counter-Terrorism White Paper, "[t]errorism has become a persistent and permanent feature of Australia's *security environment*".[43]

Government, intelligence and security publications in the United Kingdom demonstrate a similar acceptance, and use, of the concept of an environment. In *A Strong Britain in an Age of Uncertainty*, the UK Government's 2010 National Security Strategy, it is argued that "[t]he risk of major instability, insurgency or civil war overseas which creates an environment that terrorists can exploit to threaten the UK".[44] The 2008 *UK National Security Strategy* was designed "…to ensure that government thinking on national security constantly keeps pace with the rapidly evolving global *security environment*".[45] Previously, the United Kingdom's *Defence White Paper* described "…the increasingly complex *security environment* which followed the ending of the Cold War…"[46] and set out "…our analysis of the future *security environment*".[47]

Outside of government publications, the concept of a *security* or *threat environment* has been more broadly accepted and used. David Kilcullen outlines "the key features of the *threat environment*" as a means of articulating the context for his theory of *The Accidental Guerrilla*.[48] Russell Howard and Reid Sawyers' book, *Terrorism and Counterterrorism:*

[43] Department of the Prime Minister and Cabinet, *Counter-Terrorism White Paper: Securing Australia, Protecting Our Community*, Commonwealth Government of Australia, Canberra, 2010, p.7. Italics added by author.
[44] United Kingdom Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, The Stationery Office, London, October 2010, p.27.
[45] Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009, p.59. Italics added by author.
[46] Ministry of Defence, *Delivering Security in a Changing World*, The Stationery Office, London, 2003, p.2. Italics added by author.
[47] *Ibid.*, p.2. Italics added by author.
[48] David Kilcullen, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Scribe, Melbourne, 2009, p.5. Italics added by author.

Understanding the New Security Environment, is reflective of the use of the concept.[49] In presenting the idea of "full-spectrum" approach to analysis, Adrian Wolfberg maintains that such a shift is required "…to meet the broad, interrelated requirements of the current *security environment*".[50] Following the 2002 Bali bombings, Aldo Borgu claims that Australia faced a "qualitatively changed *threat environment*".[51] At the same time, Alan Dupont argues that "Australia's *security environment* is in the midst of one of the most profound and far-reaching changes in recent history".[52] Similarly, Rod Lyon makes the observation that "…the international *security environment* is undergoing transformational change, driven by an increasing level of global interconnectedness and technological diffusion".[53] In a later publication, Lyon makes the point that asymmetric threats are an "…important structural driver in the future *security environment*, regardless of the course of great-power relationships".[54]

In addition to the popularity of the concept of a threat or security environment, there exists a corresponding expectation that intelligence analysis should be able to provide an understanding of this often loosely-defined threat environment. In his review of Australia's Intelligence Community, Phillip Flood concludes that the rise of JI "…demonstrates the

---

[49] Russell Howard and Reid Sawyers (Eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, The McGraw-Hill/Dushkin, Guilford, 2004. Other examples of titles include William Carpenter and David Wiencek (Eds.), *Asian Security Handbook: Terrorism and the New Security Environment*, 3rd Edition, M.E. Sharpe, New York, 2005.

[50] Wolfberg raises the concept of "all-spectrum analysis", which assumes that the world is a mystery which defies neat answers and in which conclusions are "…permanently tentative and subject to repeated challenge and re-examination". Wolfberg contrasts this approach with "all source analysis" which he argues assumes that the world consists of puzzles to be solved. with Adrian Wolfberg, Full-Spectrum Analysis: A New Way of Thinking for a New World, *Military Review*, July-August 2006, pp.35-42, p.4. Italics added by author.

[51] Aldo Borgu, *Beyond Bali: ASPI's Strategic Assessment 2002*, Australian Strategic Policy Institute, 2002, p.13. Italics added by author.

[52] Alan Dupont, Transformation or stagnation? Rethinking Australia's defence, *Australian Journal of International Affairs*, Vol. 57, No. 1, 2003, pp. 55–76, p.55. Italics added by author.

[53] Rod Lyon, Six Challenges, in Coral Bell et al., *Scoping Studies: New thinking on security*, Australian Strategic Policy Institute, Barton, 2004, pp.15-18, p.15. Italics added by author.

[54] Rod Lyon, *Alliance Unleashed: Australia and the US in a new strategic age*, Australian Strategic Policy Institute, Barton, 2005, p.21-22. Italics added by author.

crucial importance of Australian foreign intelligence agencies being alert to shifts in the regional *security environment* and the emergence of new threats".[55] Similarly, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* called for an intelligence community that is "…able to respond nimbly to an ever-shifting *threat environment*".[56] Despite this increased usage, the meaning or definitions of what constitutes a threat environment appear to have remained largely absent. However, it is necessary to consider what is understood by the concept of an *environment* in order to critically examine whether the concept provides a useful alternative to an actor-based approach to assessing non-state threats.

An analysis of the use of the term *threat environment* indicated that there are three regular factors which appear to underpin the concept. These factors are: space, time and context. In Singer's model of threat, it is evident that aspects of time, space and context are all assumed. These factors may have been able to be assumed within the context of state-based threats in which analysts and decision-makers are likely to share a common understanding of the state. However, with non-state threats, assumptions of space, time and context appear questionable, given that, as has been discussed earlier, a shared or accurate knowledge of non-state threats is less assured.

The factor of *space* appears fundamental to the concept of a security or threat environment.[57] Most frequently, this concept of space is defined by geography, albeit with

[55] Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.42. Italics added by author.
[56] Laurence Silberman and Charles Robb, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, United States Government Printing Office, Washington, D.C., March 2005. Italics added by author.
[57] The fundamental importance of geography in conceptualising threats is evident in the distinction between *external* threats and *internal* threats, in which a state's physical borders tend to be used to as the delineating

the acknowledgement that non-state actors are not necessarily geographically constrained. References to geography are evident in descriptions of a:

- state or domestic threat environment;[58]
- regional threat environment;[59]
- transnational threat environment;[60] and
- global or international threat environment.[61]

Whilst definitions of a state and international environment are contained within the terms, what defines, or differentiates, a regional or transnational security environment are not necessarily clearly articulated. Regardless, the fundamental underpinning of these is *geography* as *space*.[62] Similar to Flynt's argument, both threat actors and referents exist within this shared space. The concept of *space* does not, however, necessarily appear to be

---

factor.

[58] For example, refer to J. Boone Bartholomees, Jr (Ed.), *US Army War College Guide to National Security Policy and Strategy*, Strategic Studies Institute, Second Ed., Carlisle, June 2006 (national security environment); and AFCEA, *Intelligence and the New National Security Environment*, October 2004, available at: www.afcea.org/mission/intel/documents/innse.pdf accessed on 16 Oct 2009.

[59] For example, refer to Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.42 (regional security environment).

[60] For example, refer to Daniel Roper, *Transnational Threats: US Military Strategy*, in Carolyn Pumphrey (Ed.), *Transnational Threats: Blending Law Enforcement and Military Strategy*, US Army War College, Strategic Studies Institute, November 2000, pp.41-49, p.45 (transnational threat environment); and Brian Reed, *A Social Network Approach to Understanding an Insurgency*, Parameters, Summer 2007, pp.19-30.

[61] For example, refer to Cabinet Office, *The National Strategy of the United Kingdom: Security in an interdependent world*, March 2008, The Stationery Office, p.59 (global security environment); Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., September 2001, p.3 ("global security environment"); Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., February 2006, p.28 ("international security environment"); Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific, Singapore, 2007, p.41 (international threat environment); and Rod Lyon, *Alliance Unleashed: Australia and the US in a new strategic age*, Australian Strategic Policy Institute, Barton, 2005, p.16 ("international security environment").

[62] There are, however, other concepts of space which can be factored into *space*, the most notable is *cyber-space* which, though not necessarily *where* one would witness a mass-casualty attack is consistently identified as a *space* in which propaganda and recruitment occurs. Whilst *cyber-attacks* have, to date, been more focussed on *mass-disruption*, criminal or information collection activity, cyber-attacks have not yet been employed as a tool for directly causing mass-casualties. Even then, the concept of geography remains important as mass-casualty attacks can only ever occur within a *physical* space as they are *physical* attacks.

linked to the *specific* location of a potential attack. Instead, the concept of space appears to cover a broader geography, due to the absence of specific information on threat actors. Consequently, within the context of an environment, space regularly defaults to that of total global geography.[63] This is evident in government's descriptions of the requirement to protect the state's citizens within and beyond state borders:

- Australia's *National Security Strategy* highlights the Government's responsibility for "[p]rotecting Australians and Australian interests both at home and abroad".[64]
- The United Kingdom's National Security Strategy emphasises the requirement "…to deal with the terrorist threat to the United Kingdom and to our citizens and interests overseas".[65]
- The *National Security Strategy of the United States of America* states that "[t]his Administration has no greater responsibility than the safety and security of the American people".[66]

Given the global distribution of citizenry, this moves the concept of an environment beyond military intelligence doctrine which perceives threat in terms of a well-defined geographic are to assess threats within. The aforementioned Governments' commitments to keeping their citizenry safe offer an environment construct based on a global scale.

---

[63] These geographic areas also appear to differ from the military IPB process, which generally addresses a specific sub-state or even state area within which a defined enemy force operates.

[64] Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008.

[65] Cabinet Office, *The National Strategy of the United Kingdom: Security in an interdependent world*, March 2008, The Stationery Office, p.26.

[66] Barack Obama, *National Security Strategy of the United States of America*, The White House, Washington, D.C., May 2010, p.4. This is consistent with previous security statements. For example, the 2002 *National Security Strategy of the United States of America* argues that "…the security environment confronting the United States today is radically different from what we have faced before. Yet the first duty of the United States Government remains what it always has been: to protect the American people and American interests". George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, p.18.

The factor of time also features in discussions of a threat or security environment. Rather than references to specific time periods (years, months, days or hours), within the context of an environment, time tends to be broadly defined between: what was; what is; and what will be. Where articulated, time is referred to in terms of: past or previous[67]; present or current[68]; and future.[69]

Perhaps the most important underlying assumption of this notion of time as a factor relates to the perception that the security environment is a dynamic one. The threat environment is often described as changing, evolving[70] and growing[71], indicating that the environment is perceived as fluid. This *evolving* and *rapidly changing* nature of the environment reinforce the importance of time. Similar to the concept of space, time is not usually defined as a specific time of an attack, as this would require knowledge of a specific threat actor. Nevertheless, a generic concept of time appears fundamental in understanding and defining this concept of an environment.

---

[67] For example, refer to Donald Rumsfeld, *Transforming the Military*, Foreign Affairs, May/Jun 2002, Vol. 81, Issue 3, pp.20-32, p.22-23. Rumsfeld states that "…the Cold War is now over and the Soviet Union is gone - and with it the familiar security environment to which our nation had grown accustomed".

[68] For example, refer to George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002, p.13 ("today's security environment"); Federal Bureau of Investigation, *Intelligence Philosophy*, at: www.fbi.gov/intelligence/philio.htm accessed 13 October 2009; Kevin Rudd, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008 ("security environment we face today"); Adrian Wolfberg, Full-Spectrum Analysis: A New Way of Thinking for a New World, *Military Review*, July-August 2006, pp.35-42, p.4 ("current security environment"); Kenneth Luikart and Georgia Ang., Transforming homeland security: Intelligence indications and warning, *Air and Space Power Journal*, Vol.17, No.2, Summer 2003, pp.69-78, p. 69 ("today's threat environment").

[69] For example, refer to Ministry of Defence, *Delivering Security in a Changing World*, The Stationery Office, London, 2003, p.1 ("future security environment"); Rod Lyon, *Alliance Unleashed: Australia and the US in a new strategic age*, Australian Strategic Policy Institute, Barton, 2005, pp.21-22 ("future security environment"); Criminal Intelligence Service Canada, *Strategic Early Warning for Criminal Intelligence: Theoretical Framework & Sentinel Methodology*, 2007, Ottawa, p.4 ("the threat environment of tomorrow").

[70] For example, see Intelligence and Security Committee, *Annual Report 2004–2005*, The Stationery Office, London, 2005, p.7.

[71] Office of the Assistant Secretary for Public Affairs, *Facing the Future: Meeting the Threats and Challenges of the 21st Century, Highlights of the Priorities, Initiatives, and Accomplishments of the US Department of Defense 2001-2004*, Department of Defense, February 2005, p.35.

Discussions using the concept of a threat environment also contain within them the often inherent assumption of a third factor, that of *context*. The context appears to be based an attempt to understand trends rather than an attempt to predict discrete events.[72] One of the most frequent descriptors used to describe the threat environment is complexity.[73] Complexity is used to describe a number of different, though potentially related, phenomena including: the diversity and scale of the numbers and types of actors that analysts need to assess (both state and non-state)[74]; the number of issues that directly threaten states; and a level of uncertainty inherent within analysis of these diverse threats.[75] A number of other frequently cited characteristics of the environment are globalisation, technological development and the diffusion of technology and weaponry.[76] Further, there is an argument that the increasingly interconnected nature of international affairs has elevated the importance local threats.[77]

---

[72] For example, the UK Government details a number of what are described as distinctive characteristics of the current threat, which are based more on broader trends than any one specific group. These characteristics are: the threat is international; terrorists are non-state actors; these groups intend to cause mass-casualties and willing to kill themselves; and terrorists are driven by extremist and violent beliefs. United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2006, p.7.

[73] In an attempt to capture the complexity of the environment, Richard Dannat uses the term "hybrid circumstances", describing two trends influencing the environment: persistent conflict and complexity of the physical, human and information "terrain". See, Transcript: General Sir Richard Dannatt, www.chathamhouse.org.uk, p.13. See also George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., March 2006, p.3; and Office of the Assistant Secretary for Public Affairs, *Facing the Future: Meeting the Threats and Challenges of the 21st Century, Highlights of the Priorities, Initiatives, and Accomplishments of the US Department of Defense 2001-2004*, Department of Defense, February 2005, p.47.

[74] For example, refer to Center for Security Studies, Emerging Threats in the 21st Century, *Strategic Foresight and Warning Seminar Series*, Final Report, Zurich, December 2007, p.12; also Joint Chiefs of Staff, *The National Military Strategy of the United States of America, A Strategy for Today; A Vision for Tomorrow*, Washington, D.C., 2004, p.viii.

[75] Refer to the George W. Bush, *National Security Strategy of the United States of America*, The White House, Washington, D.C., March 2006, p.3.

[76] For example, refer to Central Intelligence Agency, *Conference Report: Intelligence for a New Era in American Foreign Policy*, Center for the Study of Intelligence, January 2004, p.1; also Angus Houston, The ADF of the Future, *Australian Defence Force Journal*, No. 173, 2007, pp.57-67, p.62.

[77] For example, refer to Stephen Sloan, Foreword: Responding to the Threat, in Robert Bunker (Ed.), *Networks, Terrorism and Global Insurgency*, Routledge, London, 2005, p.xxi; also Center for Security Studies, "Emerging Threats in the 21st Century", *Strategic Foresight and Warning Seminar Series*, Final

In addition to frequently identified factors, a number of researchers have specifically analysed trends within the context of non-state threats. These researchers have, whether deliberately or not, moved beyond the dominant episteme to focus more broadly at trends that will influence global threats. For example, Alfred Rolington identifies three shifts within the "global culture" which he argues have had a profound impact on western intelligence: the information revolution; a shift from state security threats to corporate free market politics and globalization; and more wealthy, educated, informed and mobile populations within western societies.[78] Brynjar Lia's work, *Globalisation and the Future of Terrorism: Patterns and Predictions*, evaluates global trends of: globalisation and armed conflicts; international relations; the global market economy; demographic factors; ideological shifts; and technological innovations, analysing these within the context of their potential effects on the future of terrorism.[79] Similarly, Kevin O'Brien argues that the information revolution has directly impacted "…on the nature of the threat-actors in today's world".[80]

There is a perception that by understanding the environment (that is the space, time and context within which threat actors and referents exist and emerge), governments and security agencies are able to influence events, even without knowledge of individual threat actors. The hypothesis is that the actions, or inactions, of governments can make the

---

Report, Zurich, December 2007, p.12; and Angel Rabasa et al., Beyond al-Qaeda: The Global Jihadist Movement, RAND Corporation, Santa Monica, 2006, p.xx.

[78] Alfred Rolington, Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.738-759, p.744.

[79] Brynjar Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions*, Routledge, London, 2005, p.6.

[80] Kevin O'Brien, Information Age Terrorism and Warfare, in David Jones (Ed.), *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004, pp.127-128.

environment more hostile or more permissive to existing non-state threats and whether or not new threats emerge. For example, the Australian Department of Foreign Affairs and Trade argues that "[t]he Singapore Government's robust response to the terrorist threat means that Singapore is a hostile and dangerous operating environment for Jemaah Islamiyah and similar groups".[81] In contrast, "[p]orous borders, combined with massive inbound tourist and business flows, open immigration regimes, limited identity and document fraud detection, inadequately trained or corrupt officials, poor coordination between border control agencies and various security agencies, and limited immigration and customs control capacities all provide an environment in which terrorism can flourish".[82] Similarly, in reviewing the behaviour of the group responsible for the September 2001 attacks, the 9-11 Commission concludes that Al Qa'ida considered the United States a hospitable environment for preparations for the attacks.[83] Jenkins argues that cooperation amongst intelligence agencies and broader coalition support for US military action, have made the global environment "extremely hostile for jihadists".[84] British Government publications repeatedly refer to making the environment less-permissive and more hostile for non-state threats as part of the CONTEST strategy.[85] The strategy includes the aim of "…creating an environment hostile to those who glorify

[81] Department of Foreign Affair and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004, p.56.
[82] *Ibid.*, pp.42 and 52.
[83] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004, p.366.
[84] Brian Jenkins, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica, 2006, p.31.
[85] CONTEST is the UK's counter-terrorist strategy. The aim of CONTEST is to "…reduce the risk to the United Kingdom and its interests overseas from international terrorism, so that people can go about their lives freely and with confidence". The strategy is broken down into four elements: pursue; prevent; protect; and prepare. These are intended to cover aspects of threat from preventing attacks and preventing people from being involved in attacks through to mitigating the impact of successful attacks. Refer to United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009, pp.52-53.

terrorism and radicalise others".[86] Even before the CONTEST strategy, the UK government conceptualised counter-terrorism plans "…to make the United Kingdom a more difficult operating environment for those wishing to plan or mount attacks".[87] The idea appears to be that even if intelligence agencies are not able to specifically identify threatening groups or individuals, the actions of police and security agencies can make radicalisation of individuals and preparation and planning of mass-casualty attacks more difficult.[88] Thus, within government publications at least, there exists a perception that external influences, such as security procedures and strategies, are able to impact the nature, even existence, of non-state threats.

The frequent references to, and concerns over, so-called 'failed states' following the September 2001 attacks, highlight a perception that such areas provided permissive environments for non-state threats plan and prepare attacks.[89] In his book *Weak Links* Stewart Patrick considered this conventional wisdom about a nexus between failed states and terrorism, concluding that the reality is more complex. According to Patrick, whilst failed and collapsing states provided havens and conflict experience, transnational groups were decreasingly reliant on such states. Patrick highlights that whilst attacks had been planned from states such as Somalia and Yemen, they had also been planned in states like Germany and Spain. The findings from Patrick's research was that "[g]enerally speaking, the most attractive states for transnational terrorists are *weak but functioning* states where

[86] *Ibid.*, p.82.
[87] Cabinet Office, *The United Kingdom and The Campaign against International Terrorism: Progress Report*, 9th September 2002, p.17.
[88] Nevertheless, as observed by the UK's Intelligence and Security Committee, intelligence agencies themselves can face a difficult and hostile environment indicating that it is not simply governments who can influence the environment. Intelligence and Security Committee, *Annual Report 2003–2004*, The Stationery Report, London, 2004, p.6.
[89] For a list of references to links between terrorism and 'failed states' from US, British, Australian and Canadian Governments of various political persuasions, refer to Stewart Patrick, *Weak Links*: *Fragile States, Global Threats and International Security*, Oxford University Press, New York, 2011, pp.4-6.

state structures have not collapsed but remain minimally effective, in the context of a permissive cultural and ideological environments. Such badly governed states allow terrorists to operate relatively undisturbed from the scrutiny of local law enforcement and interdiction efforts of foreign actors, while enjoying a basic level of order and infrastructure (including communications technology, transportation, and banking services)".[90] This potentially provides an avenue for exploring the development and harbouring of threatening entities, external to the entities themselves.

As with any methodology, an environment-based approach to threat assessment does have limitations. One of the arguments against an environment approach would be the inability to provide *evidence* of threats.[91] A trend-based approach, as Brynjar Lia recognizes, "is unable to capture short-term shifts or local variations".[92] This highlights an important limitation to any model attempting to address the challenge of non-state actors, namely that "…any terrorist attack is the result of a decision by an individual or group who are not necessarily obedient instruments in a greater game ordained by social-science theory on the causes of terrorism".[93] This argument is reinforced by Thomas Quiggen's observation that:

> Accurate predictions about discrete future events are impossible. The international system is an open system and there is no control over most of the variables, nor can all of the important variables ever be known. Future types of problems can be anticipated, but discrete events cannot be predicted.[94]

---

[90] *Ibid.*, p.96.
[91] Noting that it can similarly be argued that the conventional model can also fail to produce *evidence* of the existence of threats. The argument could be made that the conventional model 'works' because threats have been identified. However, the counter to this is that any failure to identify non-state threats using the conventional approach can be argued to be evidence that the model does not work.
[92] Brynjar Lia, *Globalisation and the Future of Terrorism: Patterns and Predictions*, Routledge, London, 2005, p.7.
[93] *Ibid.*, p.7.
[94] Thomas Quiggin, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific, Singapore, 2007, pp.200-201.

Nevertheless, the concept of an environment appears to be an attempt to conceive a time, space and context beyond a single threat actor. One of the potential advantages in moving towards an environment concept of threat is to conceptually get ahead of existing or future threat actors, rather than simply reacting to identified groups' intentions and capabilities. Within the context of how Governments and commentators apply the concept of an environment, the approach appears to offer the potential to consider broader trends in threat (often on a global level) and consider whether these are applicable beyond specific groups. Further, if governments are able to influence an environment to be *less threatening* without necessarily knowing the existence or nature of threat actors, it is perhaps a concept that warrants further research. Regardless, the idea that threat actors (and referents) exist within a geographic space, time and context appears a sound approach. Similar to the vulnerability approach, adopting and clearly defining the environment within which threat actors and referents exist appears to offer a more comprehensive model of threat.

4.2.3 Situational Approach to Threat

A third alternative to the conventional approach provides the opportunity to critically engage with the underpinning assumptions of the model, namely that human behaviour is determined by a rational consideration of intentions and capabilities. Whether or not this dual-parameter perspective adequately or accurately describes how individuals' perceive themselves or make judgments is debatable. A critical aspect of this for assessing threats is the question over an individual's identity and the influence of broader group and collectives over individuals' decisions and actions. This question over individual's self-perception is the focus of much debate within identity studies.

Identity can be described as how individuals and groups define themselves.[95] David Rousseau defines social identities as "…bundles of shared values, beliefs, attitudes, norms, and roles that are used to draw a boundary between the "in group" and the "out group"."[96] Thus, how people perceive themselves influences how they perceive others, and ultimately who they consider to be threatening and non-threatening. Further, Rousseau argues that identities are multidimensional, variable, manipulatable, evolving and susceptible to human intervention.[97] This issue of the multifaceted aspects of identity is evident in Amartya Sen's work which approaches the problem of identity and behaviour from an economic perspective. Sen highlights that, in the normal course of life, individuals are simultaneously members of various groups with each of these collectives giving a person their particular identity. Identities are, therefore, plural, with none able to singularly define the individual's identity.[98] Given these many identities, "…the pursuit of private goals may well be compromised by the consideration of the goals of others in the group with whom the person has some sense of identity".[99] The plurality of identities and external influence on individuals' decision-making has resulted in critiques of conventional economic theory. In particular, Sen argues that the idea of rationality simply as the maximisation of self-interest has led to "…serious descriptive and predictive problems in economics".[100] Additionally, criticism of behavioural assumptions used in economic analysis has increased, notably the concept of the "rational economic man". This view of "…the individual as a very "private" person – unconcerned about the rest of the world – has been

[95] David Rousseau, *Identifying Threats and Threatening Identities: The Social Construction of Realism and Liberalism*, Stanford University Press, Stanford, 2006, p.23.
[96] *Ibid.*, p.12.
[97] *Ibid.*, p.210.
[98] Amartya Sen, *Identity and Violence: The Illusion of Destiny*, W.W. Norton and Company, New York, 2006, pp.4-5.
[99] Amartya Sen, *Rationality and Freedom*, The Belknap Press of Harvard University Press, Cambridge, 2002, p.215.
[100] *Ibid.*, p.23.

seen, in my judgment rightly, as both empirically unrealistic and theoretically misleading".[101] In *Identity and Violence*, Sen highlights John Donne's warning that "No man is an island entire of itself", a concept that has often been forgotten in economic theory in attempting to describe human behaviour.[102]

A key point is that factors *external* to the individual appear to be critical in shaping the individual's decisions and behaviour. Applying this to Singer's model, the assumption that human behaviour is solely determined by an individual's perception of their own intentions and capabilities appears to be overly simplistic. This emphasis on external factors influencing both perceptions of identity as well as an individual's behaviour potentially provides insight into developing a more comprehensive model of threat. An argument can be made that an individual's sense of identity and behaviour is not just a reflection of their perspective of their own intentions or capabilities. Instead, the importance of collectives and groups influencing the individual appears particularly relevant in considering threat, given that no individual *commences* life with the intention or capability to kill.

One potential avenue for developing a more comprehensive approach to identifying and assessing threats is to draw from the field of sociology, psychology and social psychology.[103] Keith Ludwick highlights the lack of progress in modelling terrorist behaviour, argues that a more comprehensive approach is to examine group dynamics, organizational motivations, and social needs to understand the impact of these dynamics on individuals to better understand how these groups develop and dissipate. Ludwick's

[101] *Ibid.*, p.213.
[102] Amartya Sen, *Identity and Violence: The Illusion of Destiny*, W.W. Norton and Company, New York, 2006, p.19.
[103] This argument is made by Marc Sageman in *Understanding Terror Networks*, University of Pennsylvania Press, Philadelphia, 2004, p.viii.

argument is to focus on groups and their influence on individual's behaviour rather than commencing with the individual; instead of looking at the "individual in the group," there is a need to look at the "group in the individual".[104]

A body of work that appears to offer potential rewards for pursuing a more comprehensive model of threat are insights into external influences on human behaviour described by the social psychologist Philip Zimbardo in *The Lucifer Effect: Understanding How Good People Turn Evil*.[105] Zimbardo's aim is to develop an understanding of the extent to which individuals are "….creatures of the situation, of the moment, of the mob" in attempting to understand how individuals can take part in massacres, mass suicide, torture and abuse.[106] According to Zimbardo, in order to understand complex behavioural patterns, there are three factors that need to be taken into account: dispositions; situations; and systems of power.[107] Zimbardo argues that most research focuses solely on dispositional factors, "…always looking first to motives, traits, genes, and personal pathologies".[108] As a consequence, there is "…a tendency both to overestimate the importance of dispositional qualities and to underestimate the importance of situational qualities when trying to understand the causes of other people's behaviour".[109] This primary focus on personal traits reflects a Western approach to prioritising the individual:

> The individual is the coin of the operating realm in virtually all of the major Western institutions of medicine, education, law, religion, and psychiatry. These institutions collectively help create the myth that individuals are always in control

[104] Keith Ludwick, *Closing the Gap: Measuring the Social Identity of Terrorists*, Naval Postgraduate School, Monterey, California, September 2008, p.2.
[105] Philip Zimbardo was involved in the well-known 1971 Stanford Prison Experiment. Details are available at: http://www.prisonexp.org/psychology/1
[106] Philip Zimbardo, *The Lucifer Effect*, Random House, New York, 2007, p.5
[107] *Ibid.*, pp.9-10.
[108] *Ibid.*, p.8.
[109] *Ibid.*, p.8.

> of their behaviour, act from free will and rational choice. Unless insane or of diminished capacity, individuals who do wrong should know that they are doing wrong and be punished accordingly. Situational factors are assumed to be little more than a set of minimally relevant extrinsic circumstances.[110]

In contrast, social psychologists:

> …tend to avoid this rush to dispositional judgement when trying to understand the causes of unusual behaviours. They prefer to begin their search for meaning by asking the "What questions": *What* conditions could be contributing to certain reactions? *What* circumstances might be involved in generating behaviour? *What* was the situation like from the perspective of the actors? Social psychologists ask: To what extent can an individual's actions be traced to factors outside the actor, to situational variables and environmental processes unique to a given setting?[111]

This "situationalist approach" attempts to provide a more comprehensive understanding of "acts of evil" such as "violence, vandalism, suicide terrorism, torture, or rape".[112] It is not that individuals are not responsible for their behaviour, but that behaviour is more likely to emerge under certain circumstances and situations.[113] Zimbardo's argues that "…situational conditions are created and shaped by higher-order factors – *systems* of power". These systems of power include institutions, power elites, situational power, social dynamics, which develop "…the lure of acceptance coupled with the threat of rejection", powerful forces in encouraging individuals obedience and compliance to the group and group norms.[114] Existing within systems of power makes it hard for individuals to act against the group because of these norms coupled with the situation. As Ervin Staub argues, "[b]eing part of a system shapes views, rewards adherence to dominant views, and

---

[110] *Ibid.*, p.320.
[111] *Ibid.*, pp.7-8.
[112] *Ibid.*, p.320.
[113] Zimbardo notes that"[a]lthough I preach the power of the situation, I also endorse the power of people to act mindfully and critically as informed agents directing their behaviour in purposeful ways. By understanding how social influence operates and realizing that any of us can be vulnerable to its subtle and pervasive powers, we can become wise and wily consumers instead of easily being influenced by authorities, group dynamics, persuasive appeals, and compliance strategies." *Ibid.*, p.21.
[114] *Ibid.*, p.259. Discussed at length in Chapters 12 and 13.

makes deviation psychology demanding and difficult".[115] Zimbardo uses the example of the holocaust in arguing how these three factors come together to influence human behaviour. According to Zimbardo, "[i]t was the interaction of personal variables of German citizens with situational opportunities provided by a System of fanatical prejudice that combined to empower so many to become willing or unwilling executioners for the state".[116] The issue is then one of human behaviour emerging out of group dynamics, situations and power systems.

This leads to a possible alternative, or more accurately *expanded*, epistemology, ontology and methodology of threat. The conventional epistemology of understanding threat based on an actor's intentions and capabilities is broadened to include factors *external* to actors, including situations, power systems and group dynamics. Similarly, an ontology of threat would be expanded beyond threat actors and referents to include the situation and power systems (which could be defined as the *social environment*) as entities within which both threat actors and referents (i.e. threatened actors) exist and emerge. This approach would move threat assessment beyond already identified individuals and groups to identifying and understanding the power structures and situations (environments) within which threats are more likely to emerge. Such an approach would potentially assist in understanding issues of radicalization, noting that individuals develop threatening intentions within a social environment. Such an approach would provide a more complex and, arguably, realistic model in assessing non-state threats. Developing any methodology to support assessments would require research and analysis, acknowledging the difficulties for people

[115] *Ibid.*, p.286.
[116] *Ibid.*, pp.287-288.

attempting to look from the outside in.[117] Nonetheless, the concerns over radicalization appear to support such efforts to identify factors which might indicate the presence or future development of threatening individuals and groups. From a methodological point of view, there do appear to be indicators or factors which indicate that threatening behaviours could emerge, with Zimbardo providing insight into two factors that appear to encourage the emergence (or at least lower the behavioural barriers) to threatening behaviour.

According to Zimbardo, two factors increase the potential for deindividuation:

> …anything, or any situation that makes people feel anonymous, as though no one knows who they are or cares to know, reduces their sense of personal accountability, thereby creating the potential for evil action. This becomes especially so when a second factor is added: if the situation or some agency gives them *permission* to engage in antisocial or violent actions against others, as in these research settings, people are ready to go to war.".[118]

Again, these external factors that potentially impact on individuals' behaviour, provide a possible approach for identifying factors that could indicate the existence or future emergence of threats. For example, "[e]nvironmental conditions contribute to making come members of society feel that they are anonymous, that no one in the dominant community knows who they are, that no one recognizes their individuality and thus their humanity. When that happens, we contribute to their transformations into potential vandals

[117] According to Zimbardo, "…it is difficult for people to appreciate fully the power of situational forces acting on individual behaviour when they are viewed outside the behavioural context." Further, he argues that "[a]t a subjective level, we can say that you have to be embedded within a situation to appreciate its transformative impact on you and others who are similarly situated. Looking in from outside won't do. Abstract knowledge of the situation, even when detailed, does not capture the affective tone of the place, its nonverbal features, its emergent norms, or the ego involvement and arousal of being a participant. It is the difference between being an audience member at a game show and being the contestant onstage". *Ibid.*, p.322.
[118] *Ibid.*, p.301.

and assassins."[119] Environments within which actors feel anonymous and diffuse responsibility appear to offer the potential for this process of deindividuation.[120] Both factors appear particularly relevant for assessing non-state threats. Non-state actors who threaten or develop into threats appear both attempting to be covert (and therefore anonymous) as well as accepting of an ideology of violent action against civilians.[121] Methodologically, identifying these factors of anonymity, reduced concern and violent ideologies appears to provide some measures or indicators that might offer insights into where threat actors exist (undetected) or are likely to emerge. Where identification of threatening actors is limited, identifying environments and situations that such actors might emerge from offers a promising field of research and the opportunity to develop a more comprehensive approach to identify and understanding threats and threat actors. Consequently, there does appear to be potential to identify potentially threatening group dynamics, situations and systems within which non-state threats might exist or emerge. Given the existence of a number of successful operations against groups preparing mass-casualty attacks, including communications of the group over lengthy periods, this provides information which could be useful in understanding how groups might radicalise, prepare and act as well as the social environments within which they emerge.[122]

[119] *Ibid.*, p.305.
[120] *Ibid.*, p.305.
[121] In considering collective violence, Roberta Senechal de la Rocher argues that "…rioting and terrorism may be defined partly by the presence of a logic of collective liability by which a group or members of an offender's group or social category are held accountable for the offender's conduct. Those held collectively liable might include, for example, a race, religion, ethnic group, nationality, political party, labor organization, family, clan, or tribe. Literally any member of a social category, including women, children, and the elderly, may be vulnerable to attack by rioters or terrorists". This idea of 'collective liability' has been particularly evident in mass-casualty attacks against civilians. Roberta Senechal de la Rocher, Collective Violence as Social Control, *Sociological Forum*, Vol.11, No.1, March 1996, pp.97-128, p.103
[122] Information within the public domain includes Operation Pendennis (Australia) and Operation Crevice (UK).

4.3 Towards a More Comprehensive Model of Threat

The approaches described provide potential alternatives to the conventional approach. However, rather than stand-alone alternatives, perhaps most appropriate is combining elements of each of these approaches to enable a more comprehensive approach to assessing non-state threat. As previously noted for a threat to exist, something must be threatened. Assessments of intentions and capabilities are assessed against something, whether or not this is deliberately defined. The vulnerability approach appears to be an effort at defining the referent of threat, which is critical in any consideration of the concept of threat. The environment approach has been used to describe a geographic space, time and context of threats, often at a global level, within which states attempt to protect their citizens. As threat actors and referents exist within an environment, this approach appears to provide a logical framework within which to identify threat actors and referents. The idea of permissive and non-permissive environments is also one which appears to offer the potential for identifying threat actors and hindering the development of future threats at the non-state level. This potentially links into a situational approach. In considering the problem of threat at the individual level, a situational approach recognises the importance of external factors, including group behaviour, on individual behaviour. This approach to threat appears to offer the potential to identify the situations and systems of power (social environment) within which individuals might be radicalised and which might point to social environments within which threats emerge. The opportunity to broaden the concept of threat would not ignore the conventional approach focussed on threat actors. Instead, a more comprehensive model would include broadened epistemological, ontological and methodological approaches aimed at assessing: the referent; geographic, temporal and context within which threat actors and referents exist; the situations within which

individuals might become threat actors; as well as intentions and capabilities where threat actors can be identified and defined, whilst acknowledging the potential limitations of this approach at the non-state level.

4.4 Puzzles, Mysteries and Complexities

Within intelligence analysis, there is an oft-referred to epistemological construct in which problems are defined as either secrets (or puzzles) and mysteries. Despite the popularity and use of this epistemological construct there has not been much development beyond the initial definition proposed by Nye. Where the concepts are used, there are often subtle yet critical differences in what defines a mystery and a secret, with the terms applied inconsistently, particularly in relation to non-state threats, highlighting the subjective use of the concepts and lack of consistent delineation between what constitutes a mystery rather than a puzzle. The discourse is confused and lacks critical debate over the application of the concepts to threat actors. Evidence suggests that distinctions between mysteries and secrets are not clear within the analytical community when considering what can and cannot be known about non-state threats.[123] Consequently, despite the use of this epistemological framework the last few decades, the conceptualisation does not appear to have shed much light over the problem of what can or cannot be known. Nevertheless, the distinction has become accepted within the intelligence profession.[124] As one author

[123] Reporting on a series of workshops considering alternative analysis techniques, Fishbein and Treverton noted that "[t]he relevance of the puzzle and mystery metaphors to transnational issues came up repeatedly in workshop discussions. Some argued that these issues were puzzles but with many of the key pieces missing. Yet it is unclear whether a puzzle that is essentially insoluble can usefully be thought of in these terms. The mystery metaphor also is problematic as it implies that one can at least assess likeliest outcomes well in advance by carefully evaluating available evidence". Warren Fishbein and Gregory Treverton, *Making Sense of Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004

[124] Loch Johnson, Preface to a Theory of Strategic Intelligence, *International Journal of Intelligence and CounterIntelligence*, Vol.16, 2003, pp.638-663, p.653.

argues, British intelligence officials are fond of intoning the "mantra" that "intelligence is about secrets, not mysteries".[125]

This concept appeared to gain popularity with Joseph Nye's 1994 Foreign Affairs article *Peering into the Future.*[126] Nye differentiated questions for intelligence into "mysteries" and "secrets", arguing that the post-Cold War had seen policymakers greater demand for answers to mysteries rather than puzzles.[127] According to Nye "[a] secret is something concrete that can be stolen by a spy or discerned by a technical sensor, such as the number of SS-12 missiles in the Soviet Union or the size of their warheads".[128] In contrast, he defined a mystery as "an abstract puzzle to which no one can be sure of the answer. For example, will Boris Yeltsin be able to control inflation in Russia a year from now? No one can steal the secret from Yeltsin. He does not know the answer".[129]

Andrew discusses this "conventional distinction" of secrets and mysteries, arguing that twentieth century Western intelligence was "good at discovering our opponents' secrets …but were more confused than we should have been by the mysteries of what they intended to do".[130] Andrew's argument appears to be that enemy's capabilities (armed forces) were secrets that were able to be understood in both World War Two and the Cold War. Mysteries, on the other hand, related to intentions, namely "…the mindset of our

[125] Davies notes that British intelligence officials often intone "the mantra that "intelligence is about secrets, not mysteries". Philip Davies, Ideas of Intelligence: Divergent National Concepts and Institutions, *Harvard International Review*, Vol.24, No.3, pp.62-66, p.63.
[126] The concept also appeared at a similar time in *Defense Intelligence Journal*
[127] Joseph Nye, Peering into the Future, *Foreign Affairs*, Vol.73, No.4, July/August 1994, pp.82-93.
[128] *Ibid.*
[129] *Ibid.*
[130] Christopher Andrew, *Intelligence analysis needs to look backwards before looking forward*, June 2004, accessed on 23 December 2008 at: www.historyandpolicy.org/

opponents – in particular, the understanding of fanaticism".[131] Lord Butler accepted this construct, arguing that "[a] hidden limitation of intelligence is its inability to transform a mystery into a secret". However, Butler's interpretation of what constituted a secret versus a mystery provides an insight into the application of the two parameters to problems. Butler argued that both an enemy's order of battle and their intentions are secrets. According to Butler, the mysteries are "what a leader truly believes, or what his reaction would be in certain circumstances". Nevertheless, he argues that the role of intelligence was to provide judgements on both secrets and mysteries.[132]

It is perhaps Gregory Treverton who has provided the greatest consideration to these epistemological constructs, and the development of his thinking over the last decade provides insight into the use and expansion of these parameters in an effort to define intelligence problems. Within Treverton's definitions and descriptions of mysteries and puzzles, there are clear temporal elements used to delineate between the two. Treverton argues that mysteries differ from puzzles in that "…puzzles have already happened. The result has occurred, though it may not yet be known".[133] In contrast, mysteries are "future and contingent, questions whose answers would-be adversaries may not want us to know but answers that they themselves do not know either".[134] In addition to temporal aspects, there are additional factors which are used in attempting to differentiate between the two categories. Treverton and Gabbard argue that "…puzzles deal less with people and more

[131] *Ibid.*
[132] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004, pp.14-15.
[133] Gregory Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge University Press, Cambridge, 2003, pp.11-12.
[134] Gregory Treverton, *Emerging Threats to National Security*, Testimony presented to the House of Representatives Permanent Select Committee on Intelligence on February 2, 2005, RAND, Santa Monica, February 2005, p.6. Again, this definition of a mystery illustrates the subtle but important differences in application, noting Lord Butler's argument that leaders' beliefs (that they should know) constitute a mystery whereas Treverton's definition of mysteries as questions that adversaries themselves do not know.

with things, such as weapon systems, munitions, technologies, and capabilities".[135] In contrast, "[a]t the end of the mystery-framing continuum would be political and societal questions related to people, such as regional issues, national intent, or group intentions and plans". Thus, according to these definitions, human behaviour is more of a mystery than a puzzle.[136] Despite this apparent clarity in delineation between secrets and mysteries, in attempting to come to grips with the challenges presented by non-state threats, Treverton and Gabbard do confuse theses distinctions. The authors argue that "…for the terrorist threat, not only can intentions not be determined by looking at capabilities, but capabilities themselves have a strong mystery element to them".[137] This is, however, inconsistent with the argument over capabilities being puzzles, and raises a number of questions. What is a "strong mystery element"? Does this mean that non-state actor's capabilities are neither secrets nor mysteries? This illustrates confusion over the definition and application of these two parameters to the problem of non-state threats. In earlier work, Fishbein and Treverton explored the use of alternative analytical techniques in assessing transnational threats. The authors referred to David Snowden's Cynefin framework for defining problems[138], comparing puzzles with Cynefin's *known* problems and mysteries to Cynefin's *knowable* problems. Fishbein and Treverton then introduced a third category "complexities", problems which "…involve some combination of the following factors: large numbers of small sized actors, fluidity of rules governing behaviour, and the large influence of situational as opposed to internal factors in shaping behaviour. Due to these characteristics, these problems can yield a wide range of sui generis outcomes that defy probabilistic

[135] Gregory Treverton; C. Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, RAND, Santa Monica, 2008, pp.3-5.
[136] *Ibid.*, pp.3-5.
[137] *Ibid.*, p.5.
[138] Refer to C. Kurtz and D. Snowden, The new dynamics of strategy: Sense-making in a complex and complicated world, *IBM Systems Journal*, Vol.42, No.3, 2003, p.468.

prediction".[139] The authors argue that complexities "…are prevalent in the transnational realm because actors are small, numerous, and relatively unbounded by rules, and processes are highly interactive".[140]

More recently, Treverton has further developed this category of complexities, arguing that complex problems "…seem particularly present in assessing terrorist groups and so protecting the homeland".[141] Treverton provides definitions of all three categories of problems: puzzles are problems which answers exist but may not be known; mysteries are problems where answers are contingent, cannot be known, but variables can be identified, along with an idea of how they combine; complexities are problems with "many actors responding to changing circumstances, not repeating any established patterns".[142] In this more comprehensive consideration of the epistemological categories, Treverton argues that complexities are similar to "wicked problems", a concept developed by Horst Rittle and Melvin Webber.[143] Treverton describes the differences between mysteries and complexities as ones of shape and "boundedness", but argues that "the mystery-complexity distinction is really a continuum". [144] However, it remains unclear where the distinctions exist or how neatly non-state threats sit within the category of complexities vice mysteries or puzzles. The actual practicalities of which aspects of threat actors can be identified and

[139] Warren Fishbein and Gregory Treverton, *Making Sense of Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004
[140] Fishbein and Treverton suggest that a state-to-state intelligence problems, such as crisis diplomacy and battlefield intelligence, is an example of a complexity, but note that "…crisis or battlefield conditions are usually time-limited or exceptional in the state-to-state realm, whereas equivalent conditions are an ongoing fact of life in the transnational realm". Warren Fishbein and Gregory Treverton, *Making Sense of Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004.
[141] Gregory Treverton, Addressing "Complexities" in Homeland Security, in Loch Johnson (Ed.), *The Oxford Handbook of National Security Intelligence*, Oxford University Press, Oxford, 2010, p.343.
[142] *Ibid*., p.344.
[143] Refer to Horst Rittel and Melvin Webber, Dilemmas in a General Theory of Planning, *Policy Sciences*, Vol.4, 1973, pp.155-169.
[144] *Ibid.*, p.347.

what cannot remains unanswered.

Accepting the puzzles, mysteries and complexities construct as it stands actually has the potential to hinder insight into what may or may not be known about non-state threats. It could quite legitimately be argued that intelligence agencies cannot be expected to identify non-state threats (including preparations for mass attacks) because the actors are too complex, their actions unpredictable or contingent on the actions of states, and potential attacks are in the future. Based on these characteristics, it could be argued that such threats are either mysteries or complexities. As Gentry notes, "[b]y definition, mysteries cannot be solved using methods of intelligence tradecraft".[145] However, groups that appear to fall into either the mystery or complexity categories *have* been identified planning and preparing attacks, and have been convicted on charges of terrorism. This was despite the fact that no attack or attempted attack was ever undertaken. That an attack might not have occurred did not excuse these individuals from preparations and convictions based on the judgement that they *would* have happened. Certainly, there is difficulty deciding on delineations between puzzles, mysteries and complexities at the non-state level when some groups and individuals have been identified and arrested preparing for attacks whereas others have managed to conduct attacks without detection. So are threats from non-state actors puzzles, mysteries or complexities? If elements of non-state threats can be defined within each category then against which criteria would these be applied?

Instead of providing insight, the acceptance of this epistemological argument by intelligence officials and analysts actually has the potential to be used in preventing critical

[145] John Gentry, Intelligence Failure Reframed, *Political Science Quarterly*, Vol.123, No.2, 2008, pp.247-270, p.251.

examination of analysis and assessments. The conclusion that people's actions are only knowable in hindsight may be accurate, but then what is the purpose of intelligence analysis? If intelligence only deals with current, physical but inanimate objects then the billions of dollars spent annually by governments across the world should perhaps be invested elsewhere. In summary, whilst these epistemological constructs have been popularised and accepted, the inability to agree on definitions and delineations between secrets, mysteries and, more recently, complexities hinders effective application to non-state threats. Whilst this approach could prove useful, there needs to be greater debate over the epistemological concepts, existing distinctions and the lack of consistent delineations with regard to understanding non-state threats.

The next three chapters each consider a successful mass-casualty attack in order to vivify the analytical challenge of non-state threats in distinct and faceted ways. The three incidents are: the September 2001 attacks on New York and Washington by Al Qa'ida; the October 2002 bombings in Bali by Jemaah Islamiyah; the July 2005 bombings in London by four individuals believed to have had links with Al Qa'ida. Following each of these attacks, formal investigations were undertaken to identify what these agencies did know about the threats and why intelligence agencies did not identify preparations for the attacks. Each investigation provided the opportunity to directly draw upon primary evidence in the form of declassified intelligence analysis, submissions from intelligence agencies, and testimonies from government officials and analysts. Consequently, each of these investigations allows insight into the practical application of Singer's model to the analysis and assessment of actual non-state threats.

These following chapters consider how analysts conceptualised threats from non-state

actors, what was known about non-state threats before these attacks, and what conclusions can be reached about the application of Singer's model within these specific incidents. As evident from these investigations, the respective intelligence agencies were applying the conventional model to assessments of non-state threats, and yet in each case missed identifying the threat which was manifest during the attacks. This raises issues of whether or not intelligence agencies and analysts can accurately identify and assess complex non-state threats and highlights the potential consequences where this cannot be achieved. By focussing on what intelligence agencies *actually* knew, this approach avoids the issue of hindsight bias, namely the belief that something evident only after the event should have been apparent before the event.[146] This analysis of actual events against Singer's model reinforces the argument that the conventional model of threat is too simplistic to capture the nature and complexity of non-state threats.

[146] For a discussion on the issue of hindsight bias in inquiries into intelligence refer to Richards Heuer, Limits of Intelligence Analysis, *Orbis*, Winter 2005, pp.75-94.

Chapter 5

Intelligence analysis and the 2001 attacks on New York and Washington

5.1 The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001

In September 2001, nineteen members of Al Qa'ida flew two hijacked planes into the two World Trade Centre buildings in New York and a third into the Pentagon in Washington, D.C. A fourth hijacked plane crashed in a field northwest of Washington D.C. following an attempt by passengers onboard to regain control of the aircraft. The attacks caused the deaths of almost 3,000 people and the total destruction of the World Trade Centre towers in front of an international audience. The attacks were the largest in the United States by a non-state actor and instantly reframed global perceptions of non-state threats.

The *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, was the first inquiry to consider the performance of the US intelligence community in relation to the attacks.[1] The inquiry was jointly conducted by Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence. Reflecting the scale of the attacks, the process represented the first time in

[1] The Joint Inquiry's remit was to:

- conduct a factual review of what the Intelligence Community knew or should have known prior to September 11, 2001, regarding the international terrorist threat to the United States, to include the scope and nature of any possible international terrorist attacks against the United States and its interests;
- identify and examine any systemic problems that may have impeded the Intelligence Community in learning of or preventing these attacks in advance; and
- make recommendations to improve the Intelligence Community's ability to identify and prevent future international terrorist attacks.

Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.1.

Congressional history that two permanent committees, one from the Senate and one from the House, had conducted a single, unified inquiry.[2] The Joint Committee (hereafter referred to simply as the Committee) commenced their work in February 2002, with the final report released in December that year. The Committee conducted a series of nine public hearings, and thirteen closed hearings, involving written submissions and verbal testimony from intelligence, defence and government officials.[3] In addition, Joint Inquiry staff conducted around 300 interviews, briefings and panel discussions and reviewed almost 500,000 pages of material.[4] As well as the 858-page final report released by the Committee, much of the testimony and submissions from intelligence and security officials and analysts to appear before the inquiry were also made publicly available. For a number of reasons, this particular inquiry has been selected as the basis for analysis, rather than the subsequent and more famous *9-11 Commission*, for a number of reasons. Unlike the broad remit of the 9-11 Commission, the Joint Inquiry was singularly focussed on the performance of the US intelligence community.[5] Further, whilst most scholarly research has focussed on the subsequent 9/11 Commission Inquiry, there has been comparatively little analysis of the testimony presented to the Joint Inquiry or the Committee's findings. Finally, the timeliness of the inquiry, which was completed just over one year after the attacks, provides insight into what intelligence agencies knew and understood immediately before and after the event.[6]

---

[2] *Ibid.*, p.1.
[3] *Ibid.*, p.2.
[4] *Ibid.*, p.2.
[5] At the time of the inquiry, the US Intelligence Community consisted of: Central Intelligence Agency (CIA); Department of the Treasury; Department of Energy; Department of State; Defense Intelligence Agency (DIA); Federal Bureau of Investigation (FBI); National Imagery Mapping Agency (NIMA); National Reconnaissance Office (NRO); National Security Agency (NSA); US Air Force Intelligence; US Army Intelligence; US Coast Guard Intelligence; US Navy Intelligence; and US Marine Corps Intelligence. Due to the nature of the attacks, the inquiry was largely focussed on the performance of the CIA, FBI, NSA and DIA.
[6] During the Joint Inquiry (and, indeed, within the Bali Bombing Inquiry and investigation into the 2005 London bombings) the terms information and intelligence often appear to be used interchangeably. As

5.2 Ontology of Threat

Before the 11 September 2001 attacks, the major concern of the intelligence community was on state-based threats, with an acknowledgement that this primary focus needed to be broadened to include a similar level of effort in looking at non-state threats.[7] Even after the Al Qa'ida attacks, it was argued that "[t]he US Intelligence Community is hard-wired to fight the Cold War, engineered in order to do a superlative job of attacking the intelligence 'targets' presented by a totalitarian superpower rival, but nowhere near as agile and responsive to vague, shifting transnational threats as we have needed it to be".[8] During the Cold War, the intelligence community was aware of non-state threats, however these tended to fit within a state-based framework, whereby attacks by non-state actors still tended to be state-sponsored.[9] During the 1990s, there was a notable change in the nature and characteristics of non-state threats, as evident in the first attack on the World Trade Centre in 1993.[10] Despite these changes in the nature of non-state threats, what the Committee concluded was that it took some time for the intelligence community to

---

discussed in Chapter 1, the definition adopted in this thesis is of *intelligence* as information which has been analysed (information + analysis) and *information* as data containing meaning (data + meaning), references for the case study use the term interchangeably. See Luciano Floridi, *Is Semantic Information Meaningful Data?*, Philosophy and Phenomenological Research, Vol LXX, No.2, March 2005, p.353.

[7] Paul Wolfowitz, *Prepared Testimony of the Deputy Secretary of Defense*, 19 September 2002, p.3, at: http://www.fas.org/irp/congress/2002_hr/091902wolfowitz.pdf. Lee Hamilton, former US Congressman, highlighted the intelligence community's primary focus on assessing the "military capabilities" of the Soviet Union during the Cold War in testimony to the Seventh Public Hearing, 3 October 2002.

[8] Senator Shelby, Additional Comments, p.27 in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002.

[9] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.4.

[10] Eleanor Hill, Joint Inquiry Staff Statement: Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001, 8 October 2002, pp.7-8, at: http://www.fas.org/irp/congress/2002_hr/100802hill.pdf

recognise these changes in threat.[11]

Testimony, submissions and the Committee's findings indicated that more often than not it was attacks, or attempted attacks, which prompted changes in the intelligence community's understanding of the threat.[12] That is, intelligence analysis appeared reactive and lagged behind the development of non-state threats.[13] The reactive nature of analysis to events was evident in consideration of the 1993 attack on the World Trade Centre. Joint Inquiry staff noted that "[i]nterviews of FBI personnel who were involved in the 1993 investigation of that attack suggest their initial confusion as to the nature of their new adversary. Arabs from countries hostile to one another worked together. In addition, they had no state sponsor – something that investigators had assumed they would eventually uncover".[14] The first bombing of the World Trade Center, however, "…led to a growing recognition in the Intelligence Community of a new type of terrorism that did not conform to the Cold War model: violent radical Islamic cells, not linked to any specific country, but united in anti-American zeal".[15] These changes were eventually captured in formal intelligence reports. A July 1995 National Intelligence Estimate that "…identified a 'new breed' of terrorist, who did not have a state sponsor, was loosely organized, favored an

[11] *Ibid.*, p.192.
[12] Refer to Eleanor Hill, *Joint Inquiry Staff Statement: Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001*, 8 October 2002, p.16, at: http://www.fas.org/irp/congress/2002_hr/100802hill.pdf
[13] This observation was debated during the inquiry. According to testimony presented, intelligence analysis either reacted to or kept pace with the threat. At no time, however, was it suggested that intelligence analysis was able to *anticipate* developments in the threat.
[14] Eleanor Hill, Joint Inquiry Staff Statement: Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001, 8 October 2002, pp.7-8, at: http://www.fas.org/irp/congress/2002_hr/100802hill.pdf
[15] Senator Shelby, Additional Comments, p.4 in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the U.S. Senate Select Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002. A group of eight people, with links to Egyptian Islamic Jihad, were arrested in New York in July 1993 for planning to landmarks in the city, including the United Nations and the Lincoln and Holland tunnels. The Committee noted that both 1993 plots had "…featured the deliberate intent to kill thousands of innocents by a group composed of different nationalities without a state sponsor, characteristics previously absent from terrorist schemes". *Ibid.*, pp.191-192.

Islamic agenda, and had an extreme penchant for violence".[16] Additionally, a 1997 White House noted that the CIA and FBI had warned that the threat was changing in two ways: it was not simply overseas, but included people and places within the United States; and that it was becoming more common to find individuals working alone or in ad hoc groups, some of whom were willing to die in conducting attacks.[17] One year later, the FBI wrote that "…loosely organized groups and ad hoc coalitions of foreigners motivated by perceived injustices, along with domestic groups and disgruntled individual American citizens – have attacked United States interests at home and abroad. They have chosen non-traditional targets and increasingly have employed nonconventional weapons".[18]

Despite the subsequent elevation of public awareness of Al Qa'ida, particularly following the 11 September attacks, it was evident that not all non-state threats were Al Qa'ida.[19] It was, however, argued that there were "…loose, interconnected and overlapping networks of Islamic extremists that make up the modern jihadist movement".[20] Ahmed Ressam, arrested in 1999 en route to Los Angeles to conduct a bombing of Los Angeles, and not a member of Al Qa'ida, indicated that cells operated independently, but were given lists of the types of targets that were approved within the broader context of international jihad.[21]

---

[16] *Ibid.*, p.193. National Intelligence Estimates are considered the most authoritative intelligence assessments released by the US Intelligence Community.

[17] George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee*, Ninth Public Hearing, 17 October 2002, at: http://www.fas.org/irp/congress/2002_hr/101702tenet.html

[18] Louis Freeh, *Statement of Louis J. Freeh, Former FBI Director, before the Joint Intelligence Committees, October 8, 2002*, written statement to Eighth Public Hearing, 08 October 2002, pp.15-16, at: http://www.fas.org/irp/congress/2002_hr/100802freeh.pdf

[19] For example, the 1995 bombing in Oklahoma by Timothy McVeigh.

[20] Senator Richard Shelby, Additional Views, p.103 in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the U.S. Senate Select Committee on Intelligence and the U.S. House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002.

[21] Michael Rolince, FBI Special Agent, *Prepared Remarks of Michael E. Rolince before the Select Committee on Intelligence United States Senate and the Permanent Select Committee on Intelligence House of Representatives*, September 20, 2002, p.1, at: http://www.fas.org/irp/congress/2002_hr/092002rolince.html

Nonetheless, it was Al Qa'ida which was responsible for the 11 September attacks, and it is the analysis of this organisation that we turn our attention.

Before the September 11 attacks, intelligence agencies did know of Al Qa'ida's existence and were concerned about the threat posed by bin Ladin's organisation to US interests.[22] Osama bin Ladin had made public, threatening statements in both 1996 and 1998. In these he had declared war on the United States and authorised the killing of US citizens (military and civilians) wherever they were across the globe.[23] The Al Qa'ida network had been identified as responsible for attacks against two US embassies in East Africa in 1998 and the USS Cole in Yemen in 2000. At the time of the September attacks, both the CIA and FBI had units established solely to monitor and assess the threat posed by the organisation and its leader.[24] The Director of Central Intelligence (DCI), George Tenet, stated that "[w]e knew, and warned, that Osama Bin Ladin and his al-Qa'ida [*sic*] organization were 'the most immediate and serious' terrorist threat to the US".[25] Nonetheless, the Committee found that "[p]rior to September 11, the Intelligence Community's understanding of al-Qa'ida [*sic*] was hampered by analytic focus and quality, particularly in terms of strategic

[22] The Inquiry concluded that both Presidents Bill Clinton and George W. Bush were aware of the concern by the CIA of the threat posed by bin Laden. In July 1999, President Clinton signed a document prepared by the CIA "…characterizing Bin Ladin's February 1998 statement as a 'de facto declaration of war' on the United States". Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.202. Deputy National Security Advisor Steve Hadley stated that "[f]rom the first days of the Bush Administration through September 2001, it conducted a senior level review of policy for dealing with al-Qa'ida". *Ibid.*, p.235.

[23] The Committee observed that "[i]n August 1996, Bin Ladin issued the first *fatwa* declaring *jihad* against the United States. A second *fatwa* in February 1998 proclaimed: "to kill the Americans and their allies – civilian and military is an individual duty for every Muslim who can do it in any country in which it is possible to do it." Bin Ladin repeated these threats in a May 1998 press interview. The bombings of the US embassies in Kenya and Tanzania followed in August". *Ibid.*, p.128.

[24] *Ibid.*, pp.4-5.

[25] George Tenet, *Director of Central Intelligence George J. Tenet's Testimony before the Joint Inquiry into Terrorist Attacks Against the United States*, Joint Investigation Into September 11th: Closed Hearing, 18 June 2002, declassified testimony at: http://www.fas.org/irp/congress/2002_hr/061802tenet.html

analysis".[26] As an example, the Committee noted that the Director of Central Intelligence (DCI) never produced a National Intelligence Estimate on the threat to the United States from Al Qa'ida. In addition, the Committee argued that "…analytic efforts to identify the scope and nature of the threat, particularly in the domestic United States, were clearly inadequate".[27] This was supported by evidence from the former National Security Advisor, Sandy Berger, who testified that the FBI's view had been that "…al-Qa'ida [*sic*] had limited capacity to operate in the United States and any presence here was under surveillance".[28] The Committee also noted what it saw as the "…slow response of the Intelligence Community to the developing transnational threat".[29]

The analytical difficulty appeared, in large part, to reflect an inability to accurately understand who and what Al Qa'ida was, beyond recognition of the public figure of leader Osama bin Ladin. Whilst Al Qa'ida was not new to analysts, the organisation as a non-state actor defied the kind of quantitative assessment which might be employed against "a superpower state-rival".[30] Instead, in the form of Al Qa'ida, intelligence analysts were faced with "a shadowy, cell-based network", the picture of which only developed slowly.[31] The analytical complexity of non-state threats was reflected in Rear Admiral Lowell Jacoby's submission to the inquiry. Jacoby acknowledged that, in the wake of the attack on the USS Cole, the intelligence community recognized that the "…threat had evolved and

[26] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.59.
[27] *Ibid.*, p.60.
[28] Sandy Berger quoted in *Ibid.*, p.26.
[29] *Ibid.*, p.36.
[30] Senator Richard Shelby, Additional Views, p.27 in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002.
[31] Samuel Berger, former National Security Advisor, written testimony, Second Public Hearing 19 September 2002, p.9, available at: http://www.fas.org/irp/congress/2002_hr/091902berger.pdf

changed in very complex ways and that our analytic approach had not kept pace with those changes".[32]

Even one year after the 11 September attacks, the size and nature of the organisation was a matter of debate and there remained limitations in the agencies' knowledge about the nature of Al Qa'ida.[33] The group was "…an exceptionally difficult target for US intelligence"[34] both to collect against and understand. The former Chief of the FBI's International Terrorism Operations Section, Michael Rolince, argued that that "Al Qaeda [*sic*] is far less a large organisation than a facilitator, sometimes orchestrator, of Islamic militants around the globe. These militants are linked by ideas and goals, not by organization structure".[35] This lack of an obvious structure and organisation made analysis difficult. The Committee noted that Al Qa'ida's "…organizational and command structures, which employ many activists who are not formal members of the organization, make it difficult to determine where al-Qa'ida ends and other radical groups begin".[36] The lack of a hierarchical, defined structure stood in marked contrast to the state-based threats

[32] Rear Admiral Lowell Jacoby, Acting Director, Defense Intelligence Agency, Statement for the Record to the Joint 9/11 Inquiry, 17 October 2002, p.1 at:
http://www.fas.org/irp/congress/2002_hr/101702jacoby.pdf. Testimony by the FBI's Assistant Director for Counterterrorism also indicated that the FBI's analysis of Al Qa'ida tended to be reactive to the threat. Refer to Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.62-63.

[33] Debates over the nature of Al Qa'ida continue. George Friedman argues that there has been "…a decade of failure in the intelligence community to understand what al Qaeda was and wasn't… The greatest failure of American intelligence was not the lack of a clear warning about 9/11 but the lack, on Sept. 12, of a clear picture of al Qaeda's global structure, capabilities, weaknesses and intentions. Without such information, implementing US policy was like piloting an airplane with faulty instruments in a snowstorm at night". George Friedman, *9/11 and the 9-Year War*, accessed on 9 September 2010 at:
http://www.stratfor.com/weekly/20100907_911_and_9_year_war?ip_auth_redirect=1

[34] Eleanor Hill, *Joint Inquiry Staff Statement, Part I*, September 18, 2002, p.13 at:
http://www.fas.org/irp/congress/2002_hr/091802hill.pdf

[35] Michael Rolince, FBI Special Agent, *Prepared Remarks of Michael E. Rolince before the Select Committee on Intelligence United States Senate and the Permanent Select Committee on Intelligence House of Representatives*, September 20, 2002, p.1, at:
http://www.fas.org/irp/congress/2002_hr/092002rolince.html

[36] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.198.

that the intelligence community's efforts had been largely focussed upon.

The inability to determine where Al Qa'ida began and ended highlights that the intelligence community's threat assessments and analysis was based upon a partial (even inaccurate) understanding of the network. If the intelligence community were unable to define the size and limits of Al Qa'ida, then how perceptive, rigorous or credible was their analysis? As an example, intelligence agencies' estimates over the size of Al Qa'ida remained vague.[37] The former FBI Director, Louis Freeh, estimated the size of Al Qa'ida as between "…10 to 25,000 Afghan war veterans who are all over the world".[38] Additionally, the intelligence community were unable to provide guidance on Al Qa'ida's financial resources or funding. The former National Coordinator for Counterterrorism, Richard Clarke, testified that the "…CIA was from 1995 to this day unable to tell us what it cost to be bin Laden, what it cost to be al-Qa'ida, how much was their annual operating budget within some parameters, where did the money come from, where did it stay when it wasn't being used, how was it transmitted".[39]

Al Qa'ida's transnational nature also added complexity and ambiguity, hindering intelligence agencies' attempts to identify the boundaries of the organisation. Al Qa'ida was involved in conducting or supporting attacks in "…the Balkans, the Caucasus, France, Ethiopia, Indonesia, Kenya, Saudi Arabia, Somalia, Spain, Tanzania, Tunisia, Uzbekistan,

[37] Even at the time of writing, the numerical strength of Al Qa'ida remains unknown. It is arguable whether such a measurement is even valid for an organisation such as Al Qa'ida. And perhaps attempting to measure the number of people in or linked to Al Qa'ida overlooks the logistics of the September 11 attacks which required small numbers of people to plan, finance and conduct.
[38] Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.
[39] Richard Clarke, testimony, quoted in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.117.

Yemen, and dozens of other countries".[40] Also highlighting the dispersed nature of the network was the assessment that operational planning for the September attacks had taken place in geographically diverse locations such as Germany, the U.A.E. and Malaysia.[41] The existence of a safe-haven for Al Qa'ida within a relatively remote and war-ravaged Afghanistan further inhibited collection and analysis of the organisation. Afghanistan provided Al Qa'ida members with a place to "…plan and prepare in relative freedom…"[42] as well as "…organize, train, proselytize, recruit, raise funds and grow into a worldwide menace".[43] In the case of the September attacks, that the Al Qa'ida operatives were non-US citizens operating within the US added further complexity to the nature of the threat.

As discussed in Chapter 3, for a threat to exist it must be in reference to something. In the case of Al Qa'ida, the referents could be identified as US interests, in particular US citizens. The inquiry argued that whilst threats had changed, "…the United States and its interests have long been prime terrorist targets".[44] Though US interests were not defined, a reading of testimony, submissions and the Committee's own conclusions, indicates that interests included citizenry (military and civilian), embassies, military bases and assets. Of these, it was apparent that the primary referent underpinning this concept was US citizens, based on the community's concern over mass-casualty attacks.[45] Whilst bin Ladin in his

[40] *Ibid.*, p.270.
[41] FBI quoted in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.131.
[42] Eleanor Hill, *Joint Inquiry Staff Statement, Part I*, September 18, 2002, p.13 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf
[43] Eleanor Hill, *Joint Inquiry Staff Statement: Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001*, 8 October 2002, pp.6-7, at: http://www.fas.org/irp/congress/2002_hr/100802hill.pdf
[44] *Ibid.*, p.3.
[45] For example, the 1999 edition of the FBI's *Terrorism in the United States* and intelligence community threat warning issued on 25 June 2001, both referred to in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress,

1998 fatwa had identified US citizens anywhere in the world as targets, the perception within the intelligence community was that mass-casualty attacks would likely occur against US citizens outside the United States.[46] For example, a December 2000 FBI report to Congress concluded that "[w]hile international terrorists have conducted attacks on US soil, these acts represent anomalies in their traditional targeting which focuses on US interests overseas".[47] In the lead-up to the September attacks, the intelligence community had not discounted attacks within the US, however "it was the general view of the Intelligence Community, in the spring and summer of 2001, that the threatened Bin Ladin attacks would most likely occur against US interests overseas".[48] Thus, the referent of threat could be defined as US citizens and interests outside the United States, specifically in the Arabian Peninsula, Israel, and Italy.[49]

Intelligence agencies provided these assessments to the government, which evidently influenced decision-makers' perceptions of the non-state threat. Former Assistant to the President for National Security Affairs, Samuel Berger, noted that "[t]he stream of threat information we received continuously from the FBI and CIA pointed overwhelmingly to attacks on US interests abroad".[50] The Deputy Secretary of State, Richard Armitage, testified that "I don't think we really had made the leap in our mind that we are no longer

---

2nd Session, December 2002, pp. 193 & 205.

[46] In 2004, it was estimated that there were around four million US citizens residing overseas. This does not appear to include US citizens travelling. Refer to United States Government Accountability Office, *2010 Census: Counting Americans Overseas as Part of the Decennial Census Would Not Be Cost-Effective*, August 2004, p.1.

[47] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.214.

[48] *Ibid.*, p.xi.

[49] June 2001 threat advisory issued by the intelligence community referred to in Eleanor Hill, *Joint Inquiry Staff Statement, Part I,* September 18, 2002, pp.22-23, at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf

[50] Samuel Berger, written testimony, Second Public Hearing 19 September 2002, p.6, available at: http://www.fas.org/irp/congress/2002_hr/091902berger.pdf

safe behind these two great oceans".[51] Consequently, the Committee concluded that "…the assumption prevailed in the US Government that attacks of the magnitude of September 11 could not happen here".[52]

5.3 Epistemology of Threat

During the course of the inquiry, it was apparent that intelligence analysts, officials and Committee members framed their judgements of threat principally in terms of assessments of intentions and capabilities. This was reflected in submissions, testimony and the Committee's final report. The Committee found that "[t]he Intelligence Community repeatedly warned that al-Qa'ida had both the capability and the intention to threaten the lives of thousands of Americans and that it wanted to strike within the United States. This information was conveyed in intelligence reports, broader intelligence assessments, counterterrorism policy documents, and classified Congressional testimony".[53] In testimony to the inquiry, former US Senator Warren Rudman observed that "…our intelligence community, as well as most foreign ones that I have studied, are extraordinarily good at looking at structure, at capability and intent".[54] Paul Wolfowitz, Deputy Secretary of Defence, spoke about threats in terms of people "…with horrible capabilities and with hostile intentions".[55] Armitage similarly reflected this dual-parameter model of threat, noting that "…bin Laden had the means and the intent to attack

[51] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.39.
[52] *Ibid.*, p.xix.
[53] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.242.
[54] Warren Rudman, former US Senator, testimony to the Eighth Public Hearing, 8 October 2002.
[55] Paul Wolfowitz, Deputy Secretary of Defence, testimony to the Second Public Hearing, 19 September 2002.

Americans".[56] Details of criteria for setting threat levels or assessing individual threats were not provided during the inquiry. However, testimony from Cofer Black, former Chief of the Counterterrorist Center (Central Intelligence Agency), provided insight into how threats were prioritised. Black argued that "[t]he highest criteria for us are terrorist groups that say they want to kill us, have the capability to kill and have killed us".[57] Testimony from policymakers in both the Clinton and Bush administrations reflected on intelligence community guidance warnings of the threat of Al Qa'ida which "…was both capable of and seeking to inflict mass casualties on America".[58] Also apparent in assessments of threat was the ongoing debate between Singer's parameters. Clarke argued that "…you can look at capabilities rather than intent, because intent changes".[59]

The Committee's acceptance, and use, of the conventional model of threat was also apparent. Indeed, the Committee's adoption and evaluation of the intelligence community's performance against this approach is evident in the final report. For example, the Committee compiled a list of what they perceived to be "Intelligence about Bin Ladin's Intentions to Strike Inside the United States". This list highlighted previous plots and attempted attacks, which the Committee argued indicated the bin Ladin's *intent* to conduct attacks in the US, noting that the US intelligence community had not provided such a list to policymakers.[60] Nonetheless, as noted above, the Committee did conclude that intelligence agencies had "…repeatedly warned that al-Qa'ida had both the capability and

[56] Testimony for Deputy Secretary of State Richard Armitage, Hearing Before the Joint Intelligence Committee, 19 September 2002.
[57] Cofer Black, testimony, 26 September 2002.
[58] Joint Inquiry Staff Statement, Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001, Eleanor Hill, Staff Director, Joint Inquiry Staff, October 8, 2002.
[59] Richard Clarke, testimony, Closed Hearing, 11 June 2002, declassified transcript, at: http://www.fas.org/irp/congress/2002_hr/061102clarke.pdf
[60] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.198-203.

the intention…" to threaten Americans.[61] This conclusion, if taken in isolation, could be taken as an indication that intelligence agencies were successful in their efforts to identify and understand the threat from Al Qa'ida. However, as previously highlighted, the Committee found that the intelligence community did *not* adequately address the transnational threat in general nor come to grips with Al Qa'ida.[62] Thus, whilst intelligence agencies did provide generic assessments of Al Qa'ida's threat against the dominant episteme, analysts were making assessments on the organisation as they understood it, not on the organisation as it was. Evidently, there was a significant difference. Therefore, whilst acknowledging that the intelligence community did assess and warn of the threat of Al Qa'ida against the dominant episteme, the Committee's earlier critiques indicate that assessments against the dominant episteme were not enough to provide an understanding of the threat.

Intelligence agencies' singular focus on the threat actor, and absence of a broader understanding or assessment of potential referents of threat, is evident in the Committee's criticism of a CIA plan developed to counter Osama bin Ladin.[63] The Committee argued that the plan: lacked an intelligence community-wide estimate of the threat posed by Osama Bin Ladin's network to the United States and to US interests overseas; and lacked attention to the threat to, and vulnerabilities of, the US homeland.[64] Similarly, the Committee reported that the FBI did not have the analytic capacity to assess US vulnerabilities, instead relying heavily on the CIA.[65] Additionally, the Committee levelled criticism at the CIA, noting that "[a]t times, the CIA ignored threat activity linked to the

[61] *Ibid.*, p.242.
[62] *Ibid.*, pp.36-60.
[63] *Ibid.*, p.44.
[64] *Ibid.*, p.44.
[65] *Ibid.*, p.247.

United States, focusing instead on radical activity overseas. For instance, one CIA officer told the Joint Inquiry in an interview that the travel of two hijackers to Los Angeles was not important and that he was interested only in their connection to Yemen".[66] The requirement to develop more comprehensive understanding of both threat and referent was captured by one Committee member who argued that the intelligence community needed to work with the newly-established Department of Homeland Security to "…match threat information with vulnerability assessments".[67]

Beyond the conventional approach to assessing threat, an alternative concept that appeared (albeit briefly) during the inquiry was that of a "threat environment". This term seemed to be applied when attempting to explain the broader context of threat. For example, when considering the arrest of Zacchias Moussaoui on suspicion of being involved in preparations for a hijacking, the Committee argued that "…no one at the FBI apparently connected the Moussaoui investigation with the heightened threat environment in the summer of 2001".[68] Additionally, the Acting Director of the Defense Intelligence Agency wrote of "…a counterterrorism mission environment characterized by pop-up threats, fleeting targets, and heavily veiled communication".[69] The use of the concept of a threat environment did illustrate, even immediately after the September 2001 attacks, the potential use of the approach to describe the broader context of non-state threats.

The intelligence community did not identifying the existence of a group within the United

[66] *Ibid.*, p.247.
[67] Representative Jane Harman, Additional Views, in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.649.
[68] *Ibid.*, p.xiii.
[69] Jacoby quoted in Senator Richard Shelby, Additional Views, in *Ibid.*, p.55.

States preparing to conduct the attacks. Additionally, before the attacks, 16 of the 19 hijackers were not known to be associated either with Al Qa'ida or any other threatening organisation.[70] The Committee considered at length the two or three hijackers who had been known to be associated with Al Qa'ida and what mistakes had led to them not being identified when in the United States.[71] However, the potential significance of most hijackers not being identified prior to the attacks escaped a similarly rigorous critique. Even so, testimonies and the final report did provide insight into why intelligence agencies lacked any information on most of the hijackers.

One of Al Qa'ida's previous tactics in preparing attacks appeared to have been to deliberately select people without obvious links to the organisation.[72] Evidence presented during the inquiry indicated the hijackers may have been selected partly due to their perceived lack of established ties to threatening organisations.[73] The potential future consequences of this tactic were not explored by the Committee, although at least one CIA analyst appeared to reflect on its significance. The National Intelligence Officer for the Near East and South Asia, Paul Pillar, argued that "[t]he intelligence target is not just a fixed set of known terrorists whose secrets we have had to try to uncover. It is anyone—even if not a card-carrying member of a known terrorist group and even if not having been involved in previous terrorist activity—who may use terrorist techniques to inflict harm on

[70] Eleanor Hill, Joint Inquiry Staff, *The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001*, September 20, 2002, p.4, at:
http://www.fas.org/irp/congress/2002_hr/092002hill.pdf
The Joint Inquiry considered Zacarias Moussaoui's arrest at length, but did not formally include him in the group as the FBI was still preparing the legal case to convict Moussaoui as the twentieth hijacker. In 2006, Zacarias Moussaoui was convicted of conspiracy to kill US citizens as part of the 11 September attacks.
[71] Refer to *Ibid.*, pp.143-154.
[72] Freeh argued that the people selected for the attacks on the US embassies in East Africa were "ordinary and non-obvious people", similar to the attack on the USS Cole. Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.
[73] *Ibid.*, p.4.

US interests".[74] The arrest of Moussaoui further highlights the difficulty in linking individuals to threatening non-state actors, even when the individuals are in custody.[75] As most of the hijackers connections to Al Qa'ida were only established after 11 September, selecting people based on a lack of known association with threatening groups appears to hinder the use of an actor-based model.

5.4 Methodology of Threat Assessment

The methodology used by analysts affected the quality of the US counterterrorism strategy and shaped how US government policymakers understood threats and made decisions.[76] In making assessments of threat, analysts used all sources of information, including satellite imagery[77], communications information[78], human source reporting[79], and individuals' confessions.[80] Additionally, publicly available information also informed analysis, as evident in references to Osama bin Ladin's publicly issued fatwas. Perhaps unsurprisingly for an intelligence community that collects an estimated one billion pieces of information per day,[81] the overwhelming volume of information was consistently highlighted by

---

[74] Paul Pillar, written testimony, *Statement of Paul R. Pillar to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence*, 8 October 2002, p.1, at: http://www.fas.org/irp/congress/2002_hr/100802pillar.pdf

[75] Moussaoui had been investigated on suspicion of preparing for a hijacking of an aircraft, and arrested for overstaying his visa, but the FBI investigation had experienced difficulty in attempting to link him to any foreign-based threatening organisation. Refer to Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.315-324.

[76] *Ibid.*, p.345.

[77] George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee*, Ninth Public Hearing, 17 October 2002, at: http://www.fas.org/irp/congress/2002_hr/101702tenet.html

[78] *Ibid.*

[79] *Ibid.*

[80] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.223.

[81] Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53.

analysts and officials as a challenge facing analysts. Samuel Berger argued that "…there were mountains of intelligence information…", noting the argument that "…we were drowning in information".[82] Louis Freeh argued that "[a]nalyzing intelligence information can be like trying to take a sip of water coming out of a fire hydrant".[83] CIA and FBI analysts interviewed during the inquiry "…reported being seriously overwhelmed by the volume of information and workload prior to September 11, 2001".[84] However, the volume of information does not necessarily equate to importance of that information, with "…the smallest piece of information my [be able to] fill in the mosaic of the organization and its plans".[85] Jacoby argued that information is contextual as "[i]nformation considered irrelevant noise by one set of analysts may provide critical clues or reveal significant relationships when subjected to analytical scrutiny by another".[86]

The fragmentary, incomplete and ambiguous nature of information was also regularly identified in testimony to the inquiry; there was a consistent description of information as incomplete, fragmentary and ambiguous in nature. Jacoby observed that "…available information is by its very nature fragmentary and episodic".[87] This was reinforced by the Special Assistant for Intelligence (DIA) who argued that "…information is by its nature is fragmentary, ambiguous and episodic".[88] A former DIA analyst, Kie Fallis, stated that

---

[82] Samuel Berger, testimony to Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, 19 September 2002.
[83] Louis Freeh, *Statement of Louis J. Freeh, Former FBI Director, before the Joint Intelligence Committees, October 8, 2002*, Eighth Public Hearing, 08 October 2002, p.8, at: http://www.fas.org/irp/congress/2002_hr/100802freeh.pdf
[84] Eleanor Hill, Joint Inquiry Staff Statement, Part I, September 18, 2002, p.13 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf
[85] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.356
[86] Rear Admiral Lowell Jacoby quoted in Senator Richard Shelby, Additional Views, in *Ibid*., p.52.
[87] Rear Admiral Lowell Jacoby, Statement for the Record for the Joint 9/11 Inquiry, 1 October 2002, p.7, at: http://www.fas.org/irp/congress/2002_hr/100102jacoby.pdf
[88] Special Assistant for Intelligence, DIA, quoted in Joint Inquiry into Intelligence Community Activities

"…most intelligence relating to terrorist groups is vague and fragmentary".[89] Paul Pillar noted the "…fragmentary and ambiguous reporting, much of it of doubtful credibility, that provides only the barest and blurriest glimpses of possible terrorist activity".[90] Thus, both the volume and nature of collected information were described as problematic for accurate and insightful analysis. What about specific information relating to the attacks on 11 September?

One of the priorities of the inquiry was to identify whether any of the intelligence agencies had any specific information that could have been used to prevent the attacks in Washington D.C. and New York.[91] The Committee concluded that the intelligence community did not have information that provided specific details or warning of the September attacks.[92] Indeed, the idea that such information could be expected to be collected was questioned. As noted by a former DIA analyst, "[t]he chance that our intelligence collectors, as good as they are, will stumble upon the who, what, where, when and how of a terrorist attack and then publish it in one or two messages is highly unlikely. Waiting for such a message is foolhardy".[93] The lack of specific information, and recognition that such information might not be forthcoming despite the community's best efforts, appears to have led to the Committee's idea of the collective significance of

---

before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.341.

[89] Kie Fallis, *Lessons Learned and Actions Taken in Past Events*, written submission to the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, p.7, at: http://www.fas.org/irp/congress/2002_hr/100802fallis.pdf

[90] Paul Pillar, written testimony, *Statement of Paul R. Pillar to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence*, 8 October 2002, p.1, at: http://www.fas.org/irp/congress/2002_hr/100802pillar.pdf

[91] *Ibid.*, p.2.

[92] *Ibid.*, p.7.

[93] Kie Fallis, *Lessons Learned and Actions Taken in Past Events*, written submission to the Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, p.7, at: http://www.fas.org/irp/congress/2002_hr/100802fallis.pdf

information.

While the Committee accepted that the intelligence community did not have specific information on the September 11 plot, it concluded that "…the Intelligence Community's analytic components failed to understand the collective significance of the information in their possession".[94] The Committee's argument appeared to be that, even without specific information on the attack, the intelligence community actually knew more than they thought they did. This argument, though debatable, is potentially supported by the intelligence community's own reporting in the months prior to the attacks. A June 2001 advisory issued by the intelligence community warned government agencies of a high probability "…of an imminent 'spectacular' terrorist attack resulting in numerous casualties against US interests abroad by Sunni extremists associated with al-Qa'ida".[95] The CIA was consistently warning decision-makers that a major attack was imminent. Clarke recalled that the "…CIA had been issuing a series of threat warnings beginning in early June saying that there was a major terrorist – al Qa'ida terrorist attack about to occur in the next couple of months".[96] Deputy Secretary of State Richard Armitage stated that "George Tenet was around town literally pounding on desks saying, something is happening, this is an unprecedented level of threat information. He didn't know where it was going to happen, but he knew that it was coming".[97] Thus, the Committee found that, despite lacking specific information, the intelligence community were "…bracing for an

[94] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.69-70.
[95] *Ibid.*, p.205.
[96] Richard Clarke, testimony, Closed Hearing, 11 June 2002, declassified transcript, at: http://www.fas.org/irp/congress/2002_hr/061102clarke.pdf
[97] Deputy Secretary of State Richard Armitage Joint Inquiry Report, p.8

imminent al-Qa'ida attack…" in the summer of 2001.[98]

Given the volume, nature and lack of specific information, we now turn our attention to the methodology used to assess the threat of a mass-casualty attack, and test this against the parameters of capability and intent. The parameters used to assess the threat from Al Qa'ida were primarily capability and intent. As already noted, the Committee found that "[t]he Intelligence Community repeatedly warned that al-Qa'ida had both the capability and the intention to threaten the lives of thousands of Americans and that it wanted to strike within the United States".[99] Nevertheless, the intelligence community did not identify the plot or group behind the 11 September attacks, thus these assessments remained generic. So what were the measures, proxy-measures and indicators that the intelligence community were relying on to identify and assess the type of threat that was manifest in September 2001?

There was no specific definition of capability provided during the course of the inquiry, despite the frequent use of the term. Where capability was deliberately considered, it was apparent that the term was applied or understood differently between officials and analysts, with capability described as both quantitative and qualitative. Perceptions that Al Qa'ida's capability was quantifiable were reflected in testimony that the organisation's capabilities could be built[100], bought[101], taken[102], dismantled[103], targeted[104] and destroyed.[105]

---

[98] *Ibid.*, p.xvii.
[99] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.242.
[100] George Tenet, Director of Central Intelligence, quoted in *Ibid.*, p.121
[101] Richard Clarke, testimony, Closed Hearing, 11 June 2002, declassified transcript, at: http://www.fas.org/irp/congress/2002_hr/061102clarke.pdf
[102] George Tenet, Director of Central Intelligence, testimony to the Ninth Public Hearing, Ninth Public Hearing, 17 October 2002.

Qualitative characteristics of Al Qa'ida's capability were evident in testimony, with a description of the organisation as a "highly capable adversary"[106] being based upon its: resilience[107]; flexible command structure[108]; long-range planning[109]; operational security[110]; imagination[111]; and use of personnel without terrorist associations.[112] Thus, both quantitative and qualitative factors were evident in the measures and proxy-measures used to assess capability.

The first measure of capability to note is that of Chemical, Biological, Radiological and Nuclear (CBRN). Despite the fact that Al Qa'ida did not use any CBRN weapons in the attacks, before 11 September, "…the only terrorist tactic on which CTC had performed strategic analysis was the use of chemical, biological, radiological and nuclear weapons because of the obvious potential for mass casualties".[113] Thus, despite the fact that Al Qa'ida did not use WMD in the attacks, this was the intelligence community's primary focus when assessing potential mass-casualty attacks. Paul Pillar argued that "…there developed a widespread tendency to equate the danger of terrorism against US interests, and particularly against the US homeland, with mass casualty CBRN attacks". Pillar noted

---

[103] *Ibid*.
[104] Warren Rudman, former US Senator, testimony to the Eighth Public Hearing, 8 Oct 2002.
[105] Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.
[106] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.196.
[107] George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee*, Ninth Public Hearing, 17 October 2002, at:
http://www.fas.org/irp/congress/2002_hr/101702tenet.html
[108] *Ibid.*, pp.196-197.
[109] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.196-197.
[110] *Ibid.*, pp.196-197.
[111] *Ibid.*, pp.196-197.
[112] *Ibid*., pp.196-197.
[113] According to the DCI, in 1999 the CIA published two detailed assessments on Al Qa'ida's CBRN capabilities. George Tenet, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee*, Ninth Public Hearing, 17 October 2002, at:
http://www.fas.org/irp/congress/2002_hr/101702tenet.html

that this was in contrast to the kind of attacks that were actually taking place and went on to observe that 11 September attacks were "…the most dramatic demonstration that one could achieve mass casualties, including in the US homeland, without using CBRN".[114]

The use of hijacked aircraft as weapons was one of the most notable aspects of the attack, and one which the Joint Inquiry considered in investigating the performance of the Intelligence Community.[115] During the seven years prior to September 2001, the intelligence community produced at least twelve reports on the potential use of airplanes being used as weapons.[116] Nevertheless, whilst aware of the potential, the community "…did not produce any specific assessment of the likelihood that terrorists would use airplanes as weapons".[117] The Committee found that "[t]he failure to consider seriously the use of aircraft as weapons may be the result of insufficient resources directed to intelligence analysis. Before September 11, CTC had forty analysts to analyze terrorism issues worldwide, with only one of its five analytic branches focused on terrorist tactics".[118] Thus, despite identifying the possibility of this tactic, the intelligence community was surprised by the actual use of planes as weapons.[119] Samuel Berger reflected this, noting his surprise in Al Qa'ida's "…ability to take box cutters and airplanes

[114] Paul Pillar, written testimony, *Statement of Paul R. Pillar to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence*, 8 October 2002, p.4, at: http://www.fas.org/irp/congress/2002_hr/100802pillar.pdf

[115] The use of suicide as a tactic was not discussed during the inquiry despite the fact that the success of the attacks required that the hijackers were willing to die in the attack.

[116] *Ibid.*, p.209. The Committee did acknowledge that "the credibility of sources was sometimes questionable and information often sketchy".

[117] Eleanor Hill, *Joint Inquiry Staff Statement, Part I*, September 18, 2002, p.26 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf

[118] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.213.

[119] This surprise was not limited to the intelligence community. The US Government, US public and the international community were also surprised by the tactic of crashing airplanes into buildings.

and turn them into weapons of mass destruction".[120]

Attempts to quantify such an unconventional weapons capability appear to be extremely difficult, particularly given the lack of any tangible measures prior to the actual hijacking. Only once the aircraft were airborne did the hijackers steal the unconventional weapon, and then only for a matter of minutes. Thus, the measure of an unconventional weapons capability appears to rely more on inference than quantification. In the absence of a direct measure of unconventional weaponry, proxy-measures appear to have been similarly limited in estimating such a capability. All that appears to have been required was: an ability to get basic weapons (box cutters) through security screening; ability to hijack an aircraft and access the cockpit; and limited flying skills. The question of how assessable (or useful) such proxy-measures would be before an actual attack is questionable. Indeed, the actions of passengers aboard United Airlines Flight 93 preventing the hijackers flying the aircraft to Washington demonstrate the fine line between capable and incapable.[121]

As with measuring a state's capability, people remain a core measure of a non-state actor's capabilities. Discussions over the sanctuary that Afghanistan provided for Al Qa'ida highlighted the central position of people in enabling Al Qa'ida to "build capability". It was argued that Afghanistan enabled Bin Ladin's operatives to meet, plan, train and identify recruits with specialised skills.[122] Conversely, the arrest of Al Qa'ida operatives in

[120] Samuel Berger, testimony to Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, 19 September 2002.

[121] As the international community is now aware of the potential for using aircraft for mass-casualty attacks, it could be argued that the willingness for passengers to fight potential attackers has actually *decreased* capability. Supporting this argument are the actions of staff and passengers in restraining Richard Reid (American Airlines flight on 22 December 2001) and Umar Abdulmutallab (Northwest Airlines flight on 25 December 2009) who attempted to ignite bombs onboard aircraft.

[122] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select*

1999 was assessed as representing a loss of capability.[123] Nevertheless, identifying the number of people in Al Qa'ida, or that the organisation might draw upon, remained problematic for the intelligence community. As mentioned earlier, the former FBI Director's observation that the organisation was somewhere between 10-25,000 illustrates the difficulty of a people-based measure of capability.[124] Even if Al Qa'ida's total numbers could have been determined, it is questionable how useful this would have been in providing a measure of the group's mass-casualty attack capability.

Only nineteen people were required to successfully conduct the attacks on 11 September. The number of people required to plan and finance the attacks would likely have been greater, but were not revealed during the inquiry.[125] Focussing on those who conducted the attacks, that just nineteen individuals caused the deaths of almost three thousand people highlights the difficulty in using estimates of total numerical strength as a measure of capability.[126] Indeed, that those involved in the attacks were not identified as being in the United States, nor as part of a group planning the attacks, mitigated against assessments of capability based upon numbers of people. Indeed, without precedent, that such a small group were capable of killing thousands of people could only have been inferred or estimated. Thus, how people are used (not simply total numbers) appears critical to any assessment of people as a measure of capability.

The technical prowess of several of the hijackers who had undertaken flying training was

---

Committee on Intelligence, 107th Congress, 2nd Session, December 2002, p.121.

[123] *Ibid.*, Appendix: Evolution of the Terrorist Threat and the US response, 1983 – 2001, p.26

[124] Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.

[125] It was not clear whether the intelligence community knew (or would likely ever know) the total number involved in planning.

[126] This represents an approximate attacker to victim ratio of 1:157. This ration remains notably higher than other mass-casualty attacks since.

touched upon during the inquiry but largely overlooked as a measure of capability. This is potentially because of the limited technical prowess required to carry out the attacks. The most significant technical prowess required appears to have been physically flying the aircraft into the World Trade Centres and Pentagon. It appeared that only five or six of the hijackers had undertaken flying training, apparently only enough to turn an aircraft into a building (or crash it into the ground when about to be overpowered by passengers).

Al Qa'ida required funds to finance the hijackers' living expenses, travel, flight training, and tickets for flights on the aircraft to be hijacked. Estimates of the total funding required to conduct the attacks illustrate how relatively small the amount of money required was. The FBI estimated that the attacks cost between $175,000 to $250,000.[127] Moreover, none of the US$109,500 wired into a bank account used by the hijackers resulted in suspicious activity reports.[128] It was not simply specific details of planning for attacks that eluded the intelligence agencies, but Al Qa'ida's finances in general. As noted by Clarke, the CIA was unable to determine the network's operating costs.[129] Thus, neither specific funding for the attack nor the organisation's finances identified, meaning that finances were of limited value as a proxy-measure of capability.

Concerns over the ready availability of capability for conducting a mass-casualty attack were evident in testimony. The Deputy Director of the CIA's Counterterrorism Centre

[127] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.140

[128] Robert Mueller, *Statement for the Record, FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry*, Closed Hearing, 25 Sep 2002, p.4, declassified statement at: http://www.fas.org/irp/congress/2002_hr/092602mueller.pdf

[129] Richard Clarke, testimony, quoted in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.117.

argued that Al Qa'ida was interested in or had trained to use "…surface-to-air missiles…use of truck bombs and car bombs…the use of aircraft, both aircraft hijackings and aircraft as weapons…the use of improvised explosive devices…the use of poisons and toxins". [130] Similarly, Clarke expressed concern over the relative ease of conducting a mass casualty attack within the US in testimony, noting that "…there really is very little stopping an al-Qa'ida cell from coming into the United States, getting the ammonium nitrate, getting a big rent-a-truck and doing an Oklahoma City-style bombing – very little stopping them".[131] Thus, the capability to conduct a mass-casualty attack is clearly available and yet, somewhat counter-intuitively, not necessarily easily measurable.

Testimony, submissions and the Committee's final report emphasised the importance of identifying intentions before the attacks. As with capability, however, there was no definition of intent provided. Instead, it can be surmised that intent related to a future desire to undertake an attack.[132] There was, however, an accepted delineation between the broader intentions of Al Qa'ida, which were assumed to be captured in Osama bin Ladin's public statements, and the specific intentions of carrying out the attacks. Evidently, specific intentions were difficult to identify whereas bin Ladin's statements were widely known.[133] Additionally, whilst intentions were discussed at length, and considered of central importance in assessing threat, the indicators upon which intent was based were not

[130] CTC Deputy Director, quoted in *Ibid.*, pp.214-215.
[131] Richard Clarke, testimony, Closed Hearing, 11 June 2002, declassified transcript, at: http://www.fas.org/irp/congress/2002_hr/061102clarke.pdf
[132] For example, the Committee's discussion on Bin Ladin's intentions related to the desire to conduct an attack within the US. Refer to Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.198-203.
[133] Recipients of the CIA's CTC threat reporting highlighted the lack of information on intentions and plans of groups in their assessments prior to 11 September. Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, Appendix Evolution of the Terrorist Threat and the US Response 1983-2001, p.46.

deliberately articulated during the inquiry.[134] Therefore, the following indicators are based upon reviewing testimony, submissions and the Committee's own findings.[135]

The importance of individuals' behaviour and actions was seen as a critical indicator of hostile intentions. Lowell Jacoby noted that "[i]n discerning terrorist intentions and to provide tactical warning, it is desperately important that we harvest and exploit more information on terrorists' pre-incident behaviour and activity".[136] Certainly, the suspicious behaviour of Moussaoui raised concerns of Pan Am employees, one of whom contacted the FBI, resulting in his subsequent arrest.[137] However, none of the observed behaviour of the nineteen hijackers raised concerns or attracted the attention of members of the general public, police or intelligence agencies. Indeed, the absence of suspicious behaviour by the hijackers (up until the actual hijacking) was consistently highlighted by intelligence officials as a reason for the group's lack of prior identification. FBI Director Robert Mueller argued that the hijackers "…gave no hint to those around them what they were about. They came lawfully. They lived lawfully. They trained lawfully. They boarded aircraft lawfully. They simply relied upon everything from the vastness of the Internet to the openness of out society to do what they wanted to do without detection".[138] On a number of occasions, the hijackers (both individually and as small groups) travelled across the United States, apparently taking surveillance flights and testing airport screening

[134] For example, refer to *Ibid.*, pp.198-203, section titled *Intelligence about Bin Ladin's Intentions to Strike Inside the United States*.
[135] Again, these can be divided into physical indicators (behaviour, associations, attacks by other groups) and verbal indicators (written and spoken words).
[136] Rear Admiral Lowell Jacoby, Acting Director, Defense Intelligence Agency, Statement for the Record to the Joint 9/11 Inquiry, 17 October 2002, p.4 at:
http://www.fas.org/irp/congress/2002_hr/101702jacoby.pdf
[137] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.23.
[138] Robert Mueller, *Statement for the Record, FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry*, Closed Hearing, 25 Sep 2002, p.14, declassified statement at:
http://www.fas.org/irp/congress/2002_hr/092602mueller.pdf

without drawing attention to themselves.[139] One year after the attacks, the FBI argued that "…we have found nothing they did while in the United States that triggered a specific response about them".[140] In terms of their physical appearance, the CIA Director observed that "[t]hey dressed in Western clothes, most shaved their beards before entering the US, and they largely avoided mosques".[141] It was not that the group did not present a threat, but that their behaviour did not match threatening behaviour anticipated by analysts. Therefore, it does not hold that behaviour and actions necessarily reveal intentions.

An assumption in testimony to the Committee was that associations with threatening groups or individuals might provide intelligence agencies with an indication of an individual's intentions. This was evident in testimony relating to one of the three hijackers that the intelligence community had been aware of before the attacks. Former Chief of the FBI's International Terrorism Operations Section, Michael Rolince, noted that "[t]he FBI possessed no information relevant to al-Mihdhar's possible involvement in a terrorist attack, but focussed on al-Mihdhar because he had attended a meeting with a key individual associated with the USS Cole bombing".[142] Consequently, the FBI assessed that al-Mihdhar's "confirmed association" with members of Al Qa'ida "…ma[de] him a risk to the national security of the United States".[143] Without the knowledge that al-Mihdhar had

[139] Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.
[140] Robert Mueller, *Statement for the Record, FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry*, Closed Hearing, 25 Sep 2002, p.2, declassified statement at: http://www.fas.org/irp/congress/2002_hr/092602mueller.pdf
[141] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.168.
[142] Michael Rolince, FBI Special Agent, *Prepared Remarks of Michael E. Rolince before the Select Committee on Intelligence United States Senate and the Permanent Select Committee on Intelligence House of Representatives*, September 20, 2002, at: http://www.fas.org/irp/congress/2002_hr/092002rolince.html
[143] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.153.

returned to the United States following an earlier visit, the FBI did not connect him with other hijackers.[144] Nonetheless, association was identified as a critical indicator in identifying intentions. Both the Central Intelligence and FBI Directors argued that the hijackers were able to avoid the attentions of the intelligence community because they "…intentionally avoided actions or associations that would have attracted law enforcement attention during their time in the United States".[145] That the hijackers were aware that Intelligence agencies look for such associations was raised in the inquiry, with the FBI noting that "[a]s far as we know, they contacted no known terrorist sympathizers in the United States".[146] Thus, association would have appeared to have been a valuable indicator of intent, albeit one with limitations. In particular, not everyone associated with a known threatening organization is necessarily themselves a threat. Additionally, despite interacting with numerous people beyond the hijacking group, one year after the attack, the FBI reported that "…we have found no one in the United States except the actual hijackers who knew of the plot".[147]

The spoken or written words of non-state threat actors were also taken as an indicator of intentions. The 1996 and 1998 fatwas issued by bin Ladin were viewed as evidence of Al Qa'ida's intention to kill Americans. Given the public statements made by bin Ladin, it was not surprising that the importance of such "declared hostile intentions" was raised in testimony.[148] There was, however, an apparent delineation between public statements as an indicator of the organisation's broad intent as opposed to discussions and communications

[144] *Ibid.*, pp.150-152.
[145] *Ibid.*, p.168.
[146] Mueller quoted in *Ibid.*, p.168.
[147] Robert Mueller, *Statement for the Record, FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry*, Closed Hearing, 25 Sep 2002, p.2, declassified statement at: http://www.fas.org/irp/congress/2002_hr/092602mueller.pdf
[148] Paul Wolfowitz, Deputy Secretary of Defence, testimony to the Second Public Hearing, 19 September 2002.

relating to planning and preparations for a specific attack. Nonetheless, written or spoken words were seen as a critical indicator of both generic and specific intentions. The difference was in the difficulty in accessing the words of those preparing specific attacks compared to the public (and generic) statements being made by Osama bin Ladin.

According to the inquiry's staff, Al Qa'ida officials were very concerned with operational security, including relying on face-to-face meetings and speaking in code to disguise details of operations.[149] The importance of communications security within Al Qa'ida was apparent, with the security precautions taken by the hijackers when in the United States enabling them to conduct "…meetings and communications without detection".[150] In communicating with each other and with supporters outside of the US, the group was found to "…have used publicly accessible Internet connections at various locations. They used a minimum of 133 different pre-paid calling cards to call from various pay phones, cell phones, and land lines".[151] Consequently, whilst words were relied upon as an indicator of intentions, the hijackers appeared to make their communications appear non-threatening and difficult to collect. As observed by Clarke, "[s]ometimes you get lucky on communications intercepts, and if you put the jigsaw puzzle together, sometimes you can see intentions, but it is not the same as having a successful human, high-level penetration".[152] This was supported by Lieutenant General Hayden, Director of NSA, who observed that "SIGINT [signals intelligence] did not provide significant intelligence to prevent other major terrorist attacks against US interests such as Khobar Towers, the East

[149] Eleanor Hill, *Joint Inquiry Staff Statement, Part I,* September 18, 2002, p.13 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf
[150] Louis Freeh, former Director FBI, testimony to the Eighth Public Hearing, 8 October 2002.
[151] *Ibid*.
[152] Richard Clarke, testimony to the Joint Investigation Into September 11th: Closed Hearing, 11 June 2002, declassified transcript, at: http://www.fas.org/irp/congress/2002_hr/061102clarke.pdf

Africa US Embassies, and USS Cole".[153] Paul Pillar argued that keeping such planning hidden only required fairly simply precautions such as not communicating through means that could be intercepted and leading living lives that did not draw attention to themselves.[154] These simple precautions successfully minimised the opportunities for the intelligence community to identify the intentions of the group.

A final indicator worth highlighting was the intelligence community's use of attacks (or attempted attacks) by non-Al Qa'ida groups as an indicator of Al Qa'ida's intentions. This was evident in the assessment that the arrest of Ahmed Ressam, involved in a plot to bomb Los Angeles airport, represented "…the single most compelling piece of evidence we had that UBL was intending to strike at us in the United States".[155] Of course, as noted by the intelligence community, Ressam was not a member of Al Qa'ida.[156] Therefore, information provided by Ressam following his arrest, appear to have been used to base assessments of Al Qa'ida's generic intentions, but would not have provided insight into the specific intentions of the 11 September hijackers. The absence of indicators of the intent to carry out the September attacks did not, however, mean that no such attack was being planned. Thus, even though the intelligence community were looking for these indications,

[153] The Committee argued that "…these arguments are somewhat belied by evidence uncovered during the Joint Inquiry that identified several instances of communications providing some specifics in terms of a timeframe and general location for terrorist activity. In addition, the FBI acquired toll records that five or six hijackers communicated extensively abroad after they arrived in the United States. The Intelligence Community had no information prior to September 11, 2001 regarding these communications, and, as a result, does not know what clues they may have contained". Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.380.

[154] Paul Pillar, written testimony, *Statement of Paul R. Pillar to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence*, 8 October 2002, p.1, at: http://www.fas.org/irp/congress/2002_hr/100802pillar.pdf

[155] George Tenet, *Director of Central Intelligence George J. Tenet's Testimony before the Joint Inquiry into Terrorist Attacks Against the United States*, Joint Investigation Into September 11th: Closed Hearing, 18 June 2002, declassified testimony at: http://www.fas.org/irp/congress/2002_hr/061802tenet.html

[156] Michael Rolince, FBI Special Agent, *Prepared Remarks of Michael E. Rolince before the Select Committee on Intelligence United States Senate and the Permanent Select Committee on Intelligence House of Representatives*, September 20, 2002, at: http://www.fas.org/irp/congress/2002_hr/092002rolince.html

none were collected that could reveal the existence of either the group or their intentions.

The *post-hoc* use of the dominant episteme of threat was evident during the inquiry, with attacks regularly being taken as evidence of an organisation's current and future capabilities and intentions. In describing the 1998 attacks on the US embassies in Kenya and Tanzania, the inquiry staff noted that "[t]he attacks showed that Bin Ladin's terrorist network was capable of carrying out very bloody, simultaneous attacks and inflicting mass casualties."[157] Similarly, the Committee observed that "…the Millennium plot, and attacks against US embassies in East Africa in 1998 revealed that global Islamic extremists were capable of reaching into the United States".[158] Certainly previous attacks influenced CTC assessments about Al Qa'ida's capabilities and intentions. Cofer Black noted that "[t]he highest criteria for us are terrorist groups that say they want to kill us, have the capability to kill and have killed us".[159]

Reassessments of Al Qa'ida's capabilities and intentions based on the 11 September attacks were also apparent. Jacoby noted that "long-held analytic assumptions about terrorist groups and their intentions, values, constraints, and methods of operation…were completely shattered on 11 September".[160] One year after the attacks, Tenet argued that "…you must make the assumption that Al Qaida [*sic*] is in an execution phase and intends

---

[157] Eleanor Hill, *Joint Inquiry Staff Statement, Part I,* September 18, 2002, p.13 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf

[158] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.79. The Millenium Plot was a plan to attack Los Angeles International Airport before the 2000 new years' celebrations. The plan was uncovered when Ahmed Ressam was arrested crossing the US-Canada border. For details, refer to: http://www.fbi.gov/about-us/history/famous-cases/millennium-plot-ahmed-ressam accessed 02 May 2011.

[159] Cofer Black, *Testimony of Cofer Black*, Fifth Public Hearing, 26 September 2002, at: http://www.fas.org/irp/congress/2002_hr/092602black.html

[160] Rear Admiral Lowell Jacoby, Acting Director, Defense Intelligence Agency, Statement for the Record to the Joint 9/11 Inquiry, 17 October 2002, p.2 at: http://www.fas.org/irp/congress/2002_hr/101702jacoby.pdf

to strike us both here and overseas. That's unambiguous, as far as I am concerned".[161] Nevertheless, a post-hoc use of the dominant episteme is questionable. Given that all Al Qa'ida attacks occurred outside the United States before 11 September, a post-hoc assessment of their capabilities and intentions would likely point to a continuation of overseas attacks.[162] Additionally, an argument can be made that Al Qa'ida actually lost capability given the use of suicide as a tactic. Further, *post-hoc* assessments did not appear to take into account the increased security procedures or intelligence efforts implemented by the United States after the September attacks and what impact these would have had on Al Qa'ida.

5.5 A More Comprehensive Model of Threat

The referent of threat was principally US citizens (and more broadly 'interests') outside the United States, consequently an attack against US citizens *inside* the United States was unexpected. The referent of threat was assumed to be external to the borders of the US, whilst still being US citizens. The significance of *where* US citizens were actually attacked, highlights the critical aspect of the referent to any appreciation of threat. Against the conventional model of threat, intelligence community did assess Al Qa'ida as being a threat to US citizens based on the parameters of *intent* and *capability*. However, according to the Committee, there was more to assessments of threat than this. There were two critical factors in respect to this: failure to accurately understand the nature of the threat

[161] George Tenet, Director of Central Intelligence, testimony to the Ninth Public Hearing, Ninth Public Hearing, 17 October 2002.

[162] This assumption was evident in a December 2000 FBI report to Congress which argued that "[w]hile international terrorists have conducted attacks on US soil, these acts represent anomalies in their traditional targeting which focuses on US interests overseas". Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.214.

actor (Al Qa'ida); and a failure to appreciate what could be defined as a broader environmental factor (transnational threats in general). Part of this failure can also be argued to have not fully considered the development of a desire to achieve mass-casualty attacks, namely the development of a violent ideology (beyond just Al Qa'ida) which sought to kill as many people as possible. The issue of permissive environment was apparent with the focus on Al Qa'ida's ability to train and plan with relative impunity within Afghanistan whilst also preparing in numerous less-permissive states (Germany and the United States), supporting Stewart Patrick's later work on the preference for weak but functional states as well as the opportunities afforded by wealthier democratic states for transnational threat actors. An additional argument on the 'permissiveness' of states against such groups also appears important. The ability to enter the US, move about freely and evade suspicion was clearly critical to the 19 hijackers. The later 9-11 Commission concluded that Al Qa'ida considered the United States a hospitable environment for preparations for the attacks.[163] This underscores that it was not simply the *internal* operations security (OPSEC) measures of the hijackers, but also the *external* environment within which they were able to travel, plan and communicate.[164] This links also to Zimbardo's argument over the combination of a violent ideology as well as environments, such as urban areas, which encourage anonymity. Of note, however, the actual radicalisation of these individuals appeared to have occurred outside the United States, with the 19 hijackers apparently committed to an attack *prior* to entering the US. These factors, both *internal* and *external* to the specific threat actor highlight the potential importance of a broader, more comprehensive approach to assessing threat.

[163] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004, p.366.

[164] The actions taken following the attack can be argued to have changed the United States into a less hospitable, non-permissive environment for such groups.

Chapter 6

Intelligence analysis and the 2002 Bali bombings

6.1 Australian Senate Inquiry into Security threats to Australians in Southeast Asia

On 12 October 2002, members of Jemaah Islamiyah (JI) detonated two bombs on the Indonesian island of Bali, a popular tourist destination. The attacks resulted in the deaths of 202 people including 88 Australians. JI used two bombs in the attacks, with the first bomb (500g-1kg of TNT) detonated by an individual in Paddy's Bar, immediately followed by the detonation of a second much larger bomb (50-150kg of TNT) in a van in the street outside the bar, in front of the Sari nightclub.[1] The bombings were the worst ever mass-casualty attacks suffered by Australians citizens (either at home or overseas) by a non-state actor. At the time, Bali was the most popular overseas destination for Australian tourists and had been considered a safe destination for decades, at least amongst the Australian travelling public. The hitherto unprecedented scale of the attack within Southeast Asia, massive loss of life, and public and government surprise prompted demands for a public inquiry.

The Australian Senate Committee on Foreign Affairs and Defence subsequently conducted an inquiry to examine what government agencies, and principally the intelligence community, knew about threats to Australian citizens in South East Asia in the lead up to October 2002. The inquiry, *Security threats to Australians in South East Asia*, was

[1] Australian Federal Police source quoted Brian Jackson *et al*., *Aptitude for Destruction Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, RAND, 2005, p.70. A third bomb was detonated outside the US consulate in Denpassar, but did not result in any casualties.

conducted over fourteen months and involved ten public hearings, at which the Committee received testimony from intelligence officials and analysts. A number of formal submissions from intelligence agencies were also provided, including declassified assessments and analysis. All testimony, submissions and the Committee's final report were placed onto the public record. This information includes over 600 pages of testimony, declassified intelligence analysis and formal responses to questions, in addition to the Committee's 224-page final report. Officials and analysts appearing before the inquiry came from three intelligence agencies: the Australian Security Intelligence Organisation (ASIO); the Defence Intelligence Organisation (DIO); and the Office of National Assessments (ONA).[2] Whilst these three groups formed only part of the Australian intelligence community, they were the only intelligence agencies which conduct analysis and assessments on threats to Australia's national interests.

6.2 Ontology of Threat

The Committee concluded that the Australian intelligence community was aware of the generic non-state threat in South East Asia before the 2002 Bali bombings, and had identified a number of pertinent characteristics of both the generic non-state threat and of JI specifically. Nonetheless, the intelligence community's recognition and identification of non-state threats had been gradual, and represented a shift from the collection and analysis

[2] The Office of National Assessments (ONA) provides strategic-level intelligence advice to the Prime Minister and Government to assist in formulating policy. ONA is also responsible for coordinating "Australia's foreign intelligence activities". The Defence Intelligence Organisation provides strategic level intelligence support to "Defence and Government decision-making and the planning and conduct of Australian Defence Force operations" with a "focus on the Asia pacific region". Whereas both ONA and DIO focus solely on foreign intelligence, ASIO has both a domestic and foreign intelligence mandate in identifying threats to Australia's national security. These threats include "…espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system, and acts of foreign interference". Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, Appendix 3. The Committee's report and all testimony and submissions provided to the inquiry are available at:
http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/index.htm

priorities of the Cold War.[3] Indeed, one analyst argued that, until 11 September 2001, his agency "…still tended to consider the principal threats to national security as emanating from the nation state…", arguing that it took both the attacks in New York and Bali "to realise that there are non-state threats to security".[4] Certainly the increased allocation in resources to collecting and analysing non-state threats *after* the 11 September 2001 and 12 October 2002 attacks were evident to the Committee.[5]

The Committee found that, from around 1999, Australian intelligence agencies had developed a growing awareness "…of the rising significance and militancy within the south-east Asian region of extremist Islamic groups".[6] Between 1999 and the attacks in October 2002, three consistent themes were apparent within intelligence agencies assessments of non-state threats: the perceived weakness of the Indonesian government[7]; the potential influence of Al Qa'ida within the region[8]; and the largely domestic focus of non-state threat actors.

The weakness of the Indonesian government was consistently identified within intelligence analysis during 2000 and 2002, and this weakness was seen as enabling the growth and development of non-state threats. In 2000, ONA released a report arguing that "…the

[3] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.10.
[4] David Wright-Neville (former ONA analyst), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 November 2003, pp.259-260.
[5] Whilst deliberately avoiding the debate of whether or not intelligence agencies devoted enough effort to non-state threats prior to 12 October 2002, the Committee did observe that "[b]efore the Bali bombings, agencies such as ASIO had nowhere near the analytical resources that subsequently have been made available to them". Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.27.
[6] *Ibid.*, p.121.
[7] *Ibid.*, p.2.
[8] DIO analysis quoted in Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.12. See also Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.2.

security apparatus that had held militant Islam in check has been gradually dismantled and Islamic jihad groups, such as those now operating in Maluku, could become a permanent threat to communal harmony elsewhere in Indonesia and a menace to elected civil authority".[9] Thus, the perception was that these groups remained internally focussed, being a threat primarily to the Indonesian government and citizens. In later 2000, ONA reported that "[a]s a consequence of Indonesia's weak condition and rising lawlessness, militant groups are becoming more assertive….[The] risk is growing that international Islamic terrorists could use local militants to set up in Indonesia networks through which to extend their influence".[10] A 2001 ONA report highlighted this continuing concern over the "…potential for growth of Islamic militancy and international Islamic terrorism, especially given the difficulties Jakarta is likely to face in restoring law and order and in engineering an economic recovery".[11]

An additional external influence on Southeast Asian non-state threats was also highlighted by intelligence agencies, namely the influence of Al Qa'ida. DIO assessed Al Qa'ida's reach within the region, arguing that it did have the potential to influence attacks by non-state "…through its support and encouragement of proxy terrorist organisations".[12] ONA engaged in joint research with US intelligence counterparts examining "…the nature and evolution of radical Islam in Southeast Asia".[13] The report, released just before the 11 September 2001 attacks in the US, identified external influences on non-state threats within Southeast Asia (particularly Indonesia) of "…fundamentalist religious ideologies

[9] *Ibid.*, p.2.
[10] *Ibid.*, p.2.
[11] *Ibid.*, p.3. DIO made a similar judgement in May 2001, assessing "Indonesia provided fertile ground for extremist groups with diverse motivations and international connections". Frank Lewincamp (Director DIO), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p. 342.
[12] DIO analysis quoted in Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.12.
[13] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.2.

and concepts, such as the global Islamic jihad, emanating from the Middle East".[14] Nonetheless, despite ongoing concerns over Al Qa'ida's influence on local organisations, the nature, characteristics and extent of Al Qa'ida's presence within Southeast Asia were not confirmed by intelligence agencies before the Bali bombings (and arguably beyond).[15]

The 11 September 2001 attacks in New York and Washington had a profound impact on how Australian intelligence agencies perceived the nature and characteristics of non-state threats.[16] The Committee found that as a direct consequence of the attacks "…Australia's intelligence collection agencies refined and redoubled their efforts. In its coordinating role, ONA convened special meetings of collectors in the aftermath of 11 September 2001 to provide guidance on terrorism collection priorities".[17] These priorities and requirements were discussed and refined at the 13 meetings of the National Intelligence Collection Requirements Committee between the 11 September 2001 attacks and the Bali bombings on 12 October 2002.[18] Additionally, the attacks in New York and Washington saw ASIO make "dramatic resource reallocations", devoting their "…resources overwhelmingly to counter-terrorism".[19] Even then, the Committee concluded that "[b]efore the Bali bombings, agencies such as ASIO had nowhere near the analytical resources that subsequently have been made available to them".[20]

---

[14] *Ibid.*, p.2.
[15] Refer to 29 April 2002 ONA report and 26 July 2002 ONA report as referred to in *Ibid.*, pp.6 & 8. Also, Australian Security Intelligence Organisation, Submission No.2, p.3.
[16] The Committee argued that that the attacks "…galvanised an even more intense effort by Western intelligence agencies, including Australia's, to tackle terrorism as a transnational, global phenomenon and to acknowledge that non-state players had established themselves as a major threat to national and regional security". Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.13.
[17] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.4.
[18] *Ibid.*, p.4.
[19] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.14.
[20] *Ibid.*, p.27.

The Committee concluded that between 2000 and the Bali bombings in October 2002, the Australian intelligence community had developed an appreciation of a number of broad characteristics of the non-state threat within Southeast Asia:

> (a) The growth of Islamic extremism in SE Asia and the movement into and across the region of people associated with terrorist groups, or with experience in the conflict in Afghanistan.
> (b) The extent to which extremists in the region, including in Indonesia, were becoming increasingly influenced by, or had links with, al-Qaeda [*sic*].
> (c) The reluctance and/or incapacity of the Indonesian government to crack down on extremists or to acknowledge the presence of international terrorists and the potential for networks to develop.
> (d) The high level of generic threat that existed to Westerners and Western interests, and that Australians were clearly not immune.
> (e) The threat was directed not only at Western economic infrastructure and diplomatic interests, but also at so-called 'soft' targets, and that this threat was posed by groups with both the capability and intent to mount attacks against such interests and targets.[21]

In relation to JI, evidence and intelligence assessments provided during the inquiry indicated that Australian intelligence agencies did not develop an accurate understanding of the nature and characteristics of the organisation prior to the October 2002 bombings. Up until December 2001, JI's existence had not been identified, thus analytic efforts were focussed on already identified non-state actors, albeit non-state actors who were primarily domestically-oriented in their goals and actions. In Indonesia, the group that appeared to attract most of the intelligence agencies' efforts was Laskar Jihad.[22] However, this situation changed in December 2001, when Singaporean authorities identified the existence of JI, when it identified and arrested members of the group planning attacks against

[21] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, pp.25-26.
[22] During the inquiry, it was suggested that agencies were fixated on already identified non-state threats. One analyst acknowledged that "…the fascination or preoccupation with Laskar Jihad was to some extent obscuring the extent to which there were other groups that were working very secretly at the time and about which we had very little intelligence reporting". Richard Gordon (former Head of the Southeast Asia Branch, Office of National Assessment), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 23 June 2004, p.522.

Western targets in Singapore.

The Singapore arrests revealed "…the unequivocal presence in the region of [JI] as a terrorist organisation, certainly inspired by and probably with substantial links to al-Qa'ida".[23] It was through the efforts of the Singaporean authorities, and their willingness to share this information with regional governments, that Australian intelligence agencies became aware of the existence of JI. Consequently, the very existence of JI was only confirmed ten months before the Bali bombings. The Director-General of ASIO, Dennis Richardson, argued that "[t]he intelligence failure in Bali was the failure to identify the transition of Jemaah Islamiyah into a terrorist organisation some time after 1996. It was not on our radar screen as a terrorist organisation before December 2001".[24] The Committee similarly concluded that "Australia's intelligence agencies did not know, before December 2001, of the existence of JI as a terrorist organisation".[25]

Once JI had been identified, Australian intelligence analysts had, unbeknownst to them, just ten months to establish an understanding of JI before the bombings in Bali. This involved establishing the history of JI, understanding who and what the organisation was, and assessing the existing and future threat the group presented. Again, in developing an understanding of JI, the importance of external influences and connections appeared to be critical. A joint ONA and ASIO report published in January 2002, based on information gained from the Singapore arrests, argued that "…it isn't known when before 1999 the JI first made contact with outside terrorists, but this contact appears to have marked the

[23] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xiv.
[24] Dennis Richardson (Director of Australian Security Intelligence Organisation), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.3.
[25] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xv.

group's transition from militant organisation into terrorist group".[26] Nonetheless, despite the assessed importance of external influences on JI, neither the details nor extent of these connections with Al Qa'ida (or other non-state threat actors) was able to be determined before the Bali bombings. Instead, assessments of connections and linkages remained largely generalised, based more on inference than specific information. As an example, in mid-2002, ONA analysts' assessment began to distinguish between Al Qa'ida operating in Indonesia with local assistance compared with "…a local capability in Indonesia that was not necessarily reliant on Al Qa'ida".[27] While analysts began to consider JI an entity separate from Al Qa'ida, this issue was not entirely resolved before the bombings.[28] This underscores the difficulty in attempting to identify, and then unravel, possible links between non-state actors.

The ASIO Director argued that the discovery of JI resulted in a surge of intelligence activity, in which the intelligence community progressed its understanding of JI.[29] The ten months between identification and the Bali bombings was spent attempting "…to find out as much as possible about JI and identifying and mapping JI as closely as possible. …[U]unfortunately we had not reached a point where we could have prevented Bali".[30] Indeed, testimony and submissions indicate that the intelligence community's understanding of JI remained extremely limited up until the Bali bombings, and arguably

[26] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.6.
[27] Richard Gordon, former Head of the Southeast Asia Branch, ONA, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 23 June 2004, p.508.
[28] DIO had made the assessment that evidence indicated that JI cells in Singapore, the Philippines and Malaysia were not Al Qa'ida-controlled cells, but likely received technical assistance from Al Qa'ida. Consequently, DIO assessed that "…there must be individual associations between JI members and Al Qa'ida…", but was unable to obtain specific evidence of this before the attacks. Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p. 3.
[29] Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p. 3.
[30] Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.161.

beyond. Less than one month before the Bali Bombings, DIO identified that "…the JI organisation is only now becoming apparent".[31] Testimony to the inquiry highlighted significant limitations in the intelligence community's understanding of JI at the time of the attacks. Testimony given by the Director of DIO, Frank Lewincamp, supported this observation. Lewincamp observed that "[w]e had very little firm evidence of JI numbers, relationships and activities during that period, so analysts were making the best judgment they could".[32] Dennis Richardson noted that whilst names of some JI members were identified, "…detailed connections between names, detailed identification of cell structures, detailed identification of intent and plans was not available".[33] Finally, ONA analyst, Bill O'Malley, said before the attacks:

> We knew nothing about the way in which they were planning it at the time, where their specific locations were, what their immediate intentions were or indeed the way in which they organised any kind of planning or potential operations among themselves. That is what we were working on - trying to get a better picture of how Jemaah Islamiyah was structured and would operate.[34]

At the time of the Bali bombings intelligence agencies had established an understanding of JI, but this remained limited, as apparent in the final reports released before the Bali bombings. Four days before the bombings, ASIO assessed that JI "…may be planning attacks against Singaporean interests and assets throughout the Southeast Asian region".[35] This assessment made no specific mention of a threat to Australia or Australian interests

---

[31] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.5.
[32] Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.55.
[33] Dennis Richardson, Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.161.
[34] William O'Malley (Assistant Director-General, Southeast Asia Branch, ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.126.
[35] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.5.

abroad, but assessed that "…the possibility that Australian interests may be directly or indirectly affected".[36] Less than one month before the Bali Bombings, DIO observed that "JI has not conducted any attacks on Western interests. Rather, previous attacks linked to JI have all focused on local South-East Asian targets".[37] Two days before the attacks, ONA released a report which argued that:

> …despite some recent arrests, substantial numbers of terrorists remain free in Southeast Asia, capable of and intent on further attacks. The report noted recent arrests but observed that terrorists in the region were proving they could stage small attacks, listing some recent incidents. It said further similar attacks are on the cards including against US targets in Indonesia. …key JI leaders, who have even bigger plans, including those who plotted the Singapore operation, are still free.[38]

The argument could be made that the attacks appeared to be out of character from what analysts understood about JI. Despite this, the group *was* preparing for such an attack. This illustrates the difference between what agencies understood JI to be compared to what JI actually was.

If non-state threats were such a high priority for intelligence agencies, why were they unable to gain an accurate understanding of JI? That JI existed outside the Australia's borders, and the attacks occurred within another state, hindered detection, collection and analysis.[39] Further adding to the difficulty was the fact that the Indonesian government did

---

[36] *Ibid.*, p.5.
[37] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on Notice 20 June 2003, p.5.
[38] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.9.
[39] The Committee noted that before the Bali bombings "[m]uch of the intelligence collection relied on electronic forms of eavesdropping, with effectively no human intelligence opportunities available on the ground. The cell-based and dispersed nature of terrorist groups made it virtually impossible to winkle out information about their activities and plans". Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia,* August 2004, p.27.

not share the concerns of Australian or Singaporean agencies' concerns over JI.[40] Indeed, the Committee concluded that the Bali bombings were in part a result of "…the incapacity, or lack of political will on the part of the Indonesian government at that time to fully acknowledge JI's presence on its soil and to act decisively against extremists".[41] Additionally, the nature and characteristics of JI, as described by intelligence analysts and officials in the course of the inquiry, highlighted additional difficulties in agencies' efforts to build an understanding of who and what JI was.

The transnational nature of JI proved problematic for analysts. JI was described as a "regionally-based network" present in Singapore, Malaysia, the Philippines, and Indonesia.[42] Within this heavily-populated region of the world, identifying small numbers of people was difficult, particularly given "…porous regional borders through which individuals could transit either undetected or ignored by local authorities".[43] Additionally, the JI's structure hindered identification and assessment[44], being described both as "fragmented"[45] and as an "almost family-like cell-based".[46] JI's recruitment strategy further hampered analysts' efforts, assembling its membership through kinship, community and religious beliefs.[47] Where members were identified, it appeared that intelligence agencies found it difficult to identify where JI began and ended. JI shared its leadership with at least one other group, Indonesian Mujahidin Council, hindering attempts to

[40] *Ibid.*, p.xv.
[41] *Ibid.*, p.xv.
[42] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on Notice 20 June 2003, p.3.
[43] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.82.
[44] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on Notice 20 June 2003, p.4.
[45] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.82.
[46] *Ibid.*, p.105.
[47] Ronald Bonighton, Deputy Secretary, Defence Intelligence and Security, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353.

delineate between non-state threats.[48]

The principal focus of the Australian intelligence community's threat assessments was on threat actors. Nonetheless, the oft-assumed referent of threat is identifiable in declassified assessments and analysts and officials' testimonies. The referent was most often described in terms of generic 'targets', which JI (or other non-state threats) were assessed to be interested in attacking. The targets were described as "Australian interests"[49] and more broadly as "Western interests".[50] The more generalised concept of Western interests reflected the perception that groups like JI were not necessarily focussed on specific Australian targets as much as generic Western targets. The types of Western interests JI appeared to be interested in targeting were assessed to be official targets such as "…embassies, armed forces units, military personnel off-duty, or ships".[51] Additionally, "soft" targets were identified, including nightclubs, hotels, bars,[52] Western schools[53] and airports.[54] DIO assessed that the "…most vulnerable and numerous of Western interests in the region are tourists and expatriate business people".[55] The identification of people as the primary component of national or Western interests was evident in testimony. When asked to define "Australian interests", the Director of ASIO defined Australian interests abroad

[48] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.4.
[49] Australian Security Intelligence Organisation Submission, Security threats to Australians in South-East Asia, Submission No.2, p.5.
[50] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.4.
[51] *Ibid.*, p.3. Proposed targets for planned attacks in Singapore included the U.S and Israeli embassies, Australian and British High Commissions and commercial buildings housing US companies. Singapore Ministry of Home Affairs, *White Paper: The Jemaah Islamiyah arrests and the threat of terrorism*, 7 January 2003, p.13.
[52] David Farmer, Senior Analyst - Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p. 434.
[53] Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p. 427.
[54] David Farmer, Senior Analyst - Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p. 434.
[55] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p. 6.

as "…everything from visiting Australian dignitaries through to the Australian official representation, Australian commercial business interests and the travelling public".[56]

The transnational nature of JI meant that possible referents of threat existed across Southeast Asia, and were not simply confined to Indonesia. DIO argued that Southeast Asia offered "…a range of soft and symbolic targets for anti-Western Islamic terrorists".[57] Similarly, Richardson argued that "…there are a whole range of Western interests in South-East Asia which terrorists could have targeted if they had so wished".[58] Intelligence agencies did produce threat assessments for individual states within Southeast Asia. Nevertheless, despite the size and diversity of the archipelagic state of Indonesia, Australian intelligence agencies provided only generic threat assessments of the threat across the entire state, with no variations, delineations or differences assessed between regions.[59] Where agencies did have specific information on threats within Indonesia, the potential referents of an attack by JI appeared to point towards Indonesia's most populated island of Java.[60] Consequently, assessments of who and what represented a potential referent of threat remained generic. The question of whether or not Bali should have been assessed differently to other parts of Indonesia, due to the large numbers of Australians travelling there, represented a significant difference between the Committee and the intelligence agencies. This disagreement appeared to be based on differing perceptions of epistemology of threat.

---

[56] Dennis Richardson, Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.5.
[57] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on Notice 20 June 2003, p. 6.
[58] Dennis Richardson, Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.460.
[59] Dennis Richardson , Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.10.
[60] Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.348.

6.3 Epistemology of Threat

Agencies submissions and analysts' testimonies to the inquiry illustrated that all three intelligence agencies defined and assessed threat using Singer's model.[61] Both ASIO and DIO provided the details of their criteria for determining threat levels, identifying capability and intent as the core parameters for assessing levels of threat. ASIO's six threat levels of threat, from *Very Low* to *High*, were based upon assessments of an organisation's "…intent and capability to threaten Australia's interests".[62] At the time of the Bali attacks, ASIO's assessed the threat at the second highest of the six levels (*High Level 2*).[63] In assessing threats to Defence personnel on peacetime duties outside Australia, DIO used seven threat levels from *Certain* to *Insignificant* which were similarly based upon assessments of an organisation or individual's "capability and intent".[64] Thus, whilst DIO defined the referent of threat more specifically than ASIO (namely Defence personnel versus ASIO's more generic definition of Australian interests), both agencies' assessments of threat were based on Singer's model. While ONA did not submit a written criteria for assessing threat, in both written and verbal evidence, its analysts consistently described threat in terms of intent and capability.[65] ONA's access to senior government decision-

[61] This contrasts with the US intelligence agencies during the Joint Inquiry into the 11 September 2001 attacks. The US intelligence agencies did not release their criteria for assessing threat. Instead, as discussed in Chapter 5, the use of the dominant episteme by US intelligence agencies was evident through examining submissions, testimony and conclusions by officials, analysts and Committee members.

[62] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A.

[63] There were two levels of *High* used by ASIO, the highest being High Level 1. High Level 2 (which was the assessment at the time of the attacks) was defined as "[c]urrent intent and capability to attack Australia's interests are established circumstantially but not confirmed by reliable intelligence". *Ibid.*, Attachment A.

[64] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on Notice 20 June 2003, pp.4 & 7. DIO also asserted that Defence intelligence agencies in the US, UK, Canada and New Zealand assessed threats in similar terms to DIO, p.6.

[65] ONA acknowledged that they defer to ASIO for threat assessments if they are working on the same subject. Kim Jones, Director-General ONA, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.76.

makers meant that the conventional approach would also have influenced government's understanding of threat.[66] The criteria used by ASIO and DIO require assessments of an organisation, with the assumption being that the organisation itself is understood. Yet, as previously highlighted, the intelligence community's knowledge and understanding of who and what JI was remained severely limited. Consequently, assessments of JI's capabilities and intentions were based upon what was known about the organisation rather than what the organisation actually was.

Whilst agencies defined threat in terms of the Singer's model, it is evident that assessments of threat were not necessarily limited to this actor-based approach. Instead, threat levels were not determined solely upon an assessment of an organisation or threat actor, despite the threat criteria indicating that they should be. ASIO, in setting threat levels, did not simply adhere to their defined criteria, instead factoring in events external to identified threatening organisations. For example, the attacks of 11 September 2001 prompted reviews of assessed threat levels, with the potential for US attacks on Al Qa'ida in Afghanistan being factored into assessments of a Medium level of threat against Australian interests within Indonesia.[67] On 28 September 2001, ASIO raised the assessed level of threat to High, based in part on publicity within Indonesia of attacks against mosques and Islamic institutions in Australia.[68] The Committee similarly argued that a number of additional factors supported ASIO's assessment of a High threat level for Indonesia, including: the announcement of Australian military personnel to Afghanistan; Osama bin

[66] When ONA arranged a face-to-face meeting with Foreign Minister Alexander Downer to brief him on the threat from JI, ONA analysts argued that JI "…had the intention, they had the capability, and getting access to the kinds of equipment they needed would be no problem". William O'Malley, Assistant Director-General, Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p. 435.
[67] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, pp.3-4.
[68] *Ibid.*, p.3.

Ladin's public reference to "crusader Australian forces"; and a recurring elevation of Australia's profile as a US ally in actions against Al Qa'ida.[69] Therefore, ASIO used factors beyond any single organisation's perceived capabilities and intentions to arrive at a broader assessment of threat.[70]

In a manner similar to the US Joint Committee into the September 2001 attacks, the Australian Senate Committee adopted the conventional approach in assessing the performance of intelligence agencies and to describe threat.[71] In assessing the community's performance, the Committee concluded that "[i]ntelligence agencies had reported that Indonesia-based terrorists had the intention and capability to mount attacks against Western interests, and that Australian interests could not be regarded as exempt from such attacks".[72] Additionally, the Committee mirrored agencies' descriptions of the threat from JI in terms of capability and intent.[73] Indeed, rather than using the opportunity to critique the dominant episteme, the Committee instead focussed on interpreting differences between existing levels of threat.[74] However, the Committee's conclusions on the lack of intelligence assessments of threats against Australians in Bali highlighted that the concept of threat is not solely reliant on an actor-based approach.

---

[69] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.28.
[70] The initial assessment of a *High* threat level was not made on the basis of an assessment of JI which was not identified until December 2001.
[71] Similarly, the DIO Director provided a critique of his agency's assessments of threat against the dominant episteme, concluding that the agency underestimated "…both the level of capability and the level of intent that Jemaah Islamiyah had to undertake major attacks against Western interests in Indonesia". Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.55.
[72] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xiv. The Committee also critiqued DIO's assessments against the dominant episteme, concluding that "DIO's reports generally conveyed a somewhat more benign view of the direct threat to Westerners in Indonesia, and of JI's capacities, if not its purposes and intent", p.26.
[73] *Ibid.*, p.21.
[74] *Ibid.*, p.104.

An entire chapter of the subsequent report was devoted to the question of whether intelligence agencies should have identified Bali as particularly attractive "soft" target prior to the bombings.[75] The Committee questioned whether the large presence of Western citizens (particularly Australians) should have been taken into account in assessments. This was a major point of contention between the Committee and intelligence agencies during the inquiry.[76] Intelligence officials repeatedly argued that, in the absence of specific information, Bali did not stand out as a greater target than anywhere else in Indonesia (or Southeast Asia). The Committee disagreed, concluding that 200,000 Australians visiting Bali every year should have been reflected in both threat assessments and travel advisories.[77] In evidence, the ASIO Director identified Australian citizens as the central referent of threat.[78] Despite this, when asked whether ASIO would pay particular attention to Bali because of the presence of large numbers of Australians, the Director responded:

> No. In counter-terrorism you are seeking to identify and target those small numbers of people and those groups that might engage in acts of terrorism. The question you asked is certainly relevant in terms of DFAT's travel advisories, health information and information relating to civil disturbances and the like. But when it comes to counter-terrorism and you are looking at Indonesia, you are seeking to go after very small numbers of people and very small groups.[79]

During testimony, the ASIO Director agreed that his agency's focus was on "bad-guys" rather than "…looking at where the Australians are and what is happening to them".[80] The

---

[75] The only mention that Bali would make an attractive target, in an ONA report of 27 September 2001, "…was not made on the basis of specific intelligence reporting, but was an assessment by an expert analyst on the basis of knowledge of Indonesian Islamic extremists' attitudes and objectives". Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.3.
[76] For a summary of intelligence officials' arguments, refer to Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, pp.107-109.
[77] *Ibid.*, p.109. Travel advisories were issued by the Department of Foreign Affairs and Trade (DFAT) based on threat assessments provided by ASIO.
[78] Dennis Richardson , Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.5.
[79] *Ibid.*, p.12.
[80] *Ibid.*, p.12.

failure of this singularly actor-based approach is evident. As discussed, intelligence agencies struggled to understand the nature and characteristics of JI and unable to clarify links with Al Qa'ida. Furthermore, they were limited in their ability to identify JI members, unable to collect specific information on JI plots, and proved unable to track individuals.[81] However, information on the location of travelling Australian citizens was publicly available. Australian intelligence agencies did not use readily available information on the location of Australian citizens to inform their assessments. The Committee put the actual number of Australians travelling to Bali at around 239,000 in 2001 and over 183,000 in 2002. In the six months before the Bali bombings, over 20,000 Australians were visiting Bali each month.[82] Despite assessing threats against Australian citizens, the fact that three in every four Australians travelling to Indonesia went to Bali was never factored into threat assessments.[83] Unlike the intelligence agencies, the Committee concluded that Bali *should* have been singled out for specific attention because of the large numbers of Australians and Westerners, the presence of hotels, nightclubs and an acknowledged desire by non-state actors to attack "soft targets".[84] Consequently, a singular focus on potential threat actors, without regard to the referent of threat, was seen as establishing only a partial understanding threat.

The concept of an environment external to specific threat actor briefly appeared during the

[81] For example, whilst Imam Samudra had been identified as a member of JI Australian intelligence agencies "…had absolutely no capability to tail him, to know where he was or to know in specific terms what he was doing". William O'Malley, Assistant Director-General, Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.124.
[82] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, pp.108-109. This contrasted with the Director ASIO's estimate of only 30-40,000 Australians travelling to Bali each year. Dennis Richardson quoted in *Ibid.*, p.108.
[83] This figure is included in the Dissenting Report, in *Ibid.*, p.132.
[84] See *Ibid.*, Chapter 4.

inquiry.[85] The most notable reference here was by ASIO, who argued that based on the political, economic and social instability within Indonesia "…it was clear that an environment existed in which links between militant Islamic extremists in Indonesia and elsewhere would most likely develop".[86] The situation was assessed to be different elsewhere. Following arrests of JI members in Singapore and Malaysia, DIO assessed that JI adherents in these two states would be "…unable or unwilling to plan or conduct operations in the current security environment".[87] The use of factors external to JI was critical due to "…the near impossibility of extracting information about (let alone from) tightly knit, cell-based groups of carefully recruited militants".[88] Thus, assessments on JI were based upon both the limited information that agencies could gain on JI, in addition to information on how these types of groups operated. These external factors included: the phenomenon of bin Ladin "global jihad"; availability of weapons and explosives across the region; porous borders; and limited domestic constraints on non-state threats.[89] Despite the dominant episteme of threat being based upon an actor's assessed intentions and capabilities, Australian intelligence agencies did appear to factor in events and influences external to JI, albeit without formally defining these.

The inability to identify JI members, or to understand the organisation as it actually was, undermined a singular use of the dominant episteme of threat. The first analysts knew about JI's planning of bombings in Bali were the attacks themselves. Only after the

[85] The Committee itself also used the term "high threat environment" when describing the situation in Indonesia. Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.113.
[86] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.3.
[87] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.4.
[88] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.105.
[89] *Ibid.*, p.105.

bombings did the combined Indonesian Police (POLRI) and Australian Federal Police (AFP) investigation reveal the identities of those involved in planning and conducting the attacks. Indeed, during the inquiry, only the identities of some of those involved in the attacks were discussed.[90] Intelligence analysts confirmed that, of those identified by the police as being involved in preparing and conducting the attacks, only some perpetrators were known to the agencies within the context of threat, while other JI members involved had never been identified by intelligence agencies.[91] The inability to identify the existence of a group planning the attacks hindered the assessment of intent and capability as such assessments were not anchored to knowledge of any group.

6.4 Methodology of Threat Assessment

The methodology used by intelligence analysts was critical in influencing decision-makers, government officials, and travel advisories which were used by the travelling public. The Committee's own review of the intelligence literature led it to conclude that intelligence is "…an arena of activity in which ambiguity and ambivalence, information and disinformation, operational and policy requirements, blind spots and flashes of insight, all jostle with one another as analysts seek to extract coherence out of chaos".[92] Whilst analysts do pursue specific information, they almost invariably settle for less, and yet are still required to make sound judgments.[93] According to the Committee, the critical work of

[90] The total number of people involved in planning, supporting and conducting the attack were not revealed during the inquiry.
[91] Refer to testimony of William O'Malley, Assistant Director-General, Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.126.
[92] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.7.
[93] Senator Hutchins, Committee Chair, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.452.

intelligence analysts was their "analytical judgements"[94]; how the intelligence agencies analysed, contextualised and interpreted information to inform decision-makers "…about the way an enemy might act or a threat unfold".[95]

These analytical judgements were based upon all sources of information, including classified information, diplomatic reporting and open source material, such as news media, think-tank reports and academic publications.[96] Whilst it was argued that during 2002, analysts were facing "…a flood of information to be interpreted, contextualised and assessed"[97], there still remained limited amounts of relevant information on JI.[98] Instead of volume, it was the nature of collected information which tended to dominate discussions on analytical judgements. The Director of DIO's description summed up the broader debate, describing collected information on JI as "fragmented", "uncorroborated", "lacking in detail", "contradictory", and resulted in very skilled analysts arriving at differing assessments.[99] Despite criticism of the lack of assessments on Bali, on the specific issue of collected information, the Committee concluded that Australian intelligence agencies "…were carrying out analyses and delivering assessments that were optimal within the bounds of the information and evidence available to them". This conclusion was based on the limited and contradictory nature of collected information on JI.[100]

William Blick, the Inspector General of Intelligence and Security, conducted a formal

[94] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004,p.4.
[95] *Ibid.*, p.104.
[96] *Ibid.*, Appendix 3.
[97] *Ibid.*, p.18.
[98] Dennis Richardson , Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.457.
[99] Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, pp.55-56.
[100] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.27.

review of all classified information available to the intelligence community prior to the Bali bombings. The purpose of his review was to determine if intelligence agencies had collected any specific information that might have warned of the Bali bombings prior to the attacks. The Committee relied on Blick's findings that "…there was no intelligence that could, either then or with the benefit of hindsight, have been shown to point to the likelihood of an attack of that kind".[101] The conclusion over the absence of specific information was not the end of the Committee's analysis. Instead, the Committee argued that the covert nature of JI meant "…it would have been extremely unlikely that agencies would find themselves suddenly in possession of specific information about a JI terrorist attack in any particular place in Indonesia".[102]

This next section considers the specific measures, proxy-measures and indicators that analysts used to assess JI's capabilities and intentions. In a fashion similar to the 11 September 2001 attacks, as intelligence agencies did not identify the group planning the attack, it is apparent that many of these measures, proxy-measures and indicators were not necessarily apparent until after the event. In addition, the inquiry provided limited details of the actual attacks, and instead focussed on more generic threat assessments. Consequently, there was only limited discussion upon which to draw conclusions on measures, proxy-measures and indicators.

Despite the reliance on assessments of capability in making assessments of threat, none of the agencies or their analysts provided definitions of 'capability'. In submissions and

[101] William Blick, Inspector General of Intelligence and Security, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.95.
[102] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.105.

testimony, capability remained undefined and generic. Analysis of the limited discussion on measures and proxy-measures used to assess threat indicated that capability was understood to be both quantitative and qualitative.

The availability of conventional weapons and explosives within the region were a critical factor used in analysts' assessments of JI's potential capabilities. Analysts' inability to identify what threatening organisations were doing led to a reliance on measures which they could assess, namely the availability of weapons and explosives within Southeast Asia generally and Indonesia specifically.[103] The types of weapons that JI might have employed were addressed in DIO reporting, which noted that "…local JI capability will restrict any attack to small arms or improvised explosive devices".[104] However, additional assessments by intelligence agencies indicated that there was more to measures of capability than simply the availability of weaponry. In early October 2002, ONA assessed that "weapons and explosives are still easily available in Southeast Asia, and many potential attackers with the requisite skills remain active".[105] DIO's insistence that "[w]eapons and explosives expertise [are] freely available in the region…" in their assessments of the potential capabilities of groups like JI highlight how weapons expertise could also be described as a measure of capability.[106] This emphasis on expertise underscored the importance of people as a measure of capability, in particular individuals with skills in planning, preparing and conducting attacks.

---

[103] William O'Malley, Assistant Director-General, Southeast Asia Branch (ONA), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.435.
[104] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.5.
[105] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.9.
[106] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.4.

The importance of people as a measure of capability was evident in DIO's assessment that "…arrests of [key JI members] have reduced JI's capability in the immediate term".[107] The corollary was that senior JI members (such as Hambali and Mas Selamat bin Kestari) who had avoided arrest were considered an important measure of the organisation's ongoing capability.[108] In addition to individuals within the organisation, JI's possible links with Al Qa'ida were also considered as important measures of the organisations capabilities. Indeed, DIO had expressed doubts over JI's capabilities, suggesting that the organisation was reliant upon external assistance to execute attacks. Consequently, JI's attack capabilities were enhanced by their "…connections with regional extremists…" and "…transnational associations to al Qaeda [*sic*] to pursue anti-Western attacks in future".[109] JI also required funding in order to conduct the attacks, meaning that finances might have been used as a proxy-measure of capability. After the attacks it was discovered that a robbery of a goldsmith's shop in Bali six weeks before the attacks potentially helped to fund the bombers.[110] Nevertheless, the use of funds as a proxy-measure of capability was notably absent from testimony and submissions, and did not appear to have been used by analysts.

There was no definition of intent provided by analysts or officials during the inquiry. Consequently, a reading of submissions and testimony indicates that intentions appeared to relate to an understanding of a group or individual's desires and plans to harm another entity. Again, as there was no identification of plans to conduct the attacks that took place

[107] *Ibid.*, p. 5.
[108] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.6.
[109] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p. 5.
[110] Refer to Dissenting Report, Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.142.

in Bali, it was apparent that a number of these indicators were evident only after the attack. Based on how intentions were described, and the assessments that agencies released, there were a number of consistent indicators that analysts used in attempting to assess JI's intentions.

The actions and behaviour of JI members was an important indicator of intent, evident in testimony and assessments of the difficulty in observing such indicators. Assessments of intentions based on observable behaviour proved problematic because, as one official noted, JI members "…look like ordinary people going about their everyday business".[111] Indeed, in the wake of arrests of JI members, DIO assessed that members of covert groups throughout Southeast Asia would modify their behaviour to avoid the attentions of security forces.[112] Where JI members were arrested, namely in Singapore, it was evident that the potential targets considered by the specific cell in Singapore were taken as indicating JI's broader intentions, evident in DIO analysis. DIO argued that before the Bali bombings the evidence of JI's targeting priorities indicated that JI was interested in official or symbolic Western, but principally US, targets, including "…embassies, military assets or concentrations of US servicemen, branches of Western companies".[113] These represented the potential targets that the JI cell in Singapore had been considering for attack[114], with the conclusion that "soft" targets such as tourists were perceived to be a lower priority for JI.[115] Additionally, actual attacks influenced assessments, with JI's "…history of terrorist

[111] Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353.
[112] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to questions on notice 20 June 2003, p.4.
[113] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to questions on notice 28 May 2004, pp.9-10.
[114] Refer to Singapore Ministry of Home Affairs, *White Paper: The Jemaah Islamiyah arrests and the threat of terrorism*, 7 January 2003, p.13.
[115] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to

activity in the region" taken as an indicator of intentions to conduct further attacks.[116]

Public statements by Al Qa'ida leaders were used as an indicator of generic intentions, even assessed as possibly containing coded messages used to promote or trigger attacks. This was evident in ASIO's rationale for releasing a threat assessment two days before the Bali bombings based on concern over statements by Osama bin Ladin and Ayman al-Zawahiri in early October 2002. ASIO assessed that these statements by Osama bin Ladin and al-Zawahiri suggested "…another large scale attack or attacks by al-Qa'ida are being prepared".[117] Over one year after the attacks, ASIO analysts remained unable to determine whether the broadcasts by Al Qa'ida leaders were in any way related to the JI attacks in Bali.[118] Whilst analysts relied on JI's "declared intentions"[119], no analysts or officials made reference to any public statements made by JI prior to the bombings.

Communications between members were also seen as key indicators of specific intentions, however these proved difficult, if not impossible, to collect. The Committee noted that "[m]uch of the intelligence collection relied on electronic forms of eavesdropping", but concluded that "[t]he cell-based and dispersed nature of terrorist groups made it virtually impossible to winkle out information about their activities and plans".[120] Intelligence officials and analysts stressed in testimony "…the near impossibility of extracting information about (let alone from) tightly knit, cell-based groups of carefully recruited militants, who combined modern telephony and internet with traditional, direct word-of-

---

questions on notice 28 May 2004, p.10.
[116] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.5.
[117] *Ibid.*, p.5.
[118] *Ibid.*, p.6.
[119] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.105.
[120] *Ibid.*, p.27.

mouth communications".[121] As one official noted, covert groups like JI used cover terms in communications. Consequently, members of these groups "…are not talking about attacks and bombings; they are talking about parties, celebrations and good news. So it is very difficult to get the information in the first place, before anyone even starts assessing it".[122] Therefore, the importance of words as an indicator of intentions was undermined by agencies' inability to collect unambiguous statements of hostile intentions due to JI's careful communications. There was one area in which agencies did have success in collecting spoken and written words of JI members; interviews with arrested JI members. Information from JI members arrested in Singapore and detainees elsewhere in Southeast Asia led to increased concerns within intelligence agencies over non-state threats across the region.[123] Outside of arrested JI members, the Committee found that Australian intelligence agencies had "effectively no human intelligence opportunities on the ground".[124] This lack of access to unambiguous statements between members of the group appeared to hinder the acquisition of indicators of intentions.

The *post-hoc* use of intent and capability was evident in intelligence assessments and conclusions of Committee members.[125] A DIO report prepared six days after the Bali bombings revealed how the attacks influenced and changed the assessments of JI's capability and intent. The report argued that "[t]he Bali bombings demonstrated an intent

---

[121] *Ibid.*, p.105.
[122] Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353.
[123] Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission, p.6. Arrests of Al Qa'ida members were similarly used as souces of information on Al Qa'ida within the region. Refer to Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to questions on notice 20 June 2003, p.4.
[124] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.27.
[125] When considering the September 2001 attacks in the US, Committee members argued that these attacks warned "…the world of the reach, intent and capability of extremist Islamic terrorism". Dissenting Report, in *Ibid.*, p.129.

and capability to cause high civilian casualties not seen before in South-East Asia. Islamic extremists in South-East Asia - both individuals and groups - now have a new benchmark on which to plan attacks against domestic and Western interests".[126] Nonetheless, such a post-hoc approach does not necessarily lead analysts to accurate assessments. Prior to the Bali attacks, post-hoc assessments of JI's capabilities and intentions produced a very different conclusion.

In September 2002, DIO noted in its reporting that "JI has not conducted any attacks on Western interests. Rather, previous attacks linked to JI have all focused on local South-East Asian targets".[127] If one was to consider *post-hoc* analysis of the location of previous attacks, then there had been no previous bombings in Bali by JI or any other group prior to October 2002.[128] Additionally, previous attacks by non-state actors in both Indonesia and Southeast Asia had all been comparatively small.[129] As DIO argued in responding to questions from Committee members, the Bali bombings were "…the first mass-casualty terrorist attack in South-East Asia directly targeting Westerners or Western interests".[130] Thus, in advance of the Bali bombings, the *post-hoc* use of intentions and capabilities based on previous JI attacks would not have suggested either an intent or capability to conduct a large-scale mass-casualty attack primarily against foreign citizens in Bali. Yet this is what actually occurred, illustrating that previous attacks are not necessarily a valid measure or indicator of a group's current or future capabilities or intentions.

---

[126] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on notice 20 June 2003, p.5.
[127] *Ibid.*, p.5.
[128] Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.349
[129] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia,* Answers to Questions on notice 20 June 2003, pp.1&5.
[130] *Ibid.*, p.1.

6.5 A More Comprehensive Model of Threat

A consideration of the threat as presented in the Bali attacks, there appears to be elements of the threat that lend themselves to a more comprehensive model of threat proposed in Chapter 4. These appear in both the assessments of intelligence agencies prior to the attacks, the threat actors themselves, and the conclusions of the Senate Committee. Of note, some (though not all) of these factors do appear to have influenced considerations of threat, but were not formally articulated in threat assessment criteria, hindering the development of a more comprehensive conceptualisation of threat. The threat-actor focus of intelligence analysts resulted in the referent of threat, though definable in terms of Australian citizens, not being factored into threat assessments. As noted already, this was despite the purpose of assessments being to assess threat *against* citizens. Consequently, a more comprehensive model of threat would include knowledge of citizens as referents of threat. Without such consideration, threat assessments remained country-wide and generic, despite sub-state threat actors' actual attacks against sub-state referents (i.e. Indonesian citizens) and potential to violently threaten sub-state referents (i.e. Australian citizens). The threat actors being pursued were admittedly at the level of individuals without the identification of referents at a similar level of fidelity. It can be argued that, despite not being acknowledged, an environmental approach was being applied by Australian intelligence analysts. This was evident in their setting threat levels based on broad factors of concern including: the Indonesian government's unwillingness or inability to act against non-state threats (hence providing a permissive environment); popularity of concepts such as "global Islamic jihad" (as a violent ideology); freedom of movement of people across the region (anonymity); availability of weapons and explosives; and negative reporting of Australia within the region. Consequently, the assessed threat level was *High*, irrespective of identification of threatening groups. These factors potentially warrant additional

research in considering broader environmental factors, external to both groups and individuals. These factors could also be seen within the context of a situational approach within which individuals were radicalised, something that intelligence agencies appeared to be cognisant of, but which were not formally factor into threat assessment criteria or guidance. Without such deliberate consideration, the risk is that such factors are not consistently considered or applied in assessments of non-state threat.

Chapter 7

Intelligence analysis and the 2005 London bombings

7.1 Investigations into the 7 July 2005 bombings

The 7 July 2005 attacks in London resulted in the deaths of 56 people, including the four British citizens who carried out the bombings. That such an attack *could* occur was not incomprehensible, particularly following attacks on the rail network in Madrid the year before. Nevertheless, the specific attacks on 7 July were a surprise to the public and to the UK's intelligence community, who knew nothing of the preparations for the attack or of a group planning them. This case study on the 2005 London attacks draws upon three separate reports which came out of investigations into the attacks and the performance of intelligence and security agencies. Despite pressure to conduct a formal inquiry into the bombings, the Government instead requested the nation's Intelligence and Security Committee (ISC) to conduct an investigation into intelligence matters relevant to the attacks.[1] In May 2006, the ISC released the *Report into the London Terrorist Attacks on 7 July 2005*. In the same month, the UK's Home Office released the findings of its investigation into the 2005 London bombings, *Report of the Official Account of the Bombings in London on 7th July 2005*. In 2009, the ISC released a second report into the bombings, *Could 7/7 Have Been Prevented? Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*.[2] This report was based on the results of ongoing

[1] The ISC was established in 1994 under the Intelligence Services Act to examine the "…policy, administration and expenditure of the Security Service, Secret Intelligence Service (SIS) and Government Communications Headquarters (GCHQ)". Since its inception, the ISC has expanded its oversight "…to include examination of the work of the Joint Intelligence Committee (JIC); the Intelligence and Security Secretariat, which includes the Assessments Staff, in the Cabinet Office; and the Defence Intelligence Staff (DIS), part of the Ministry of Defence". Intelligence and Security Committee, *Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, May 2006, p.iv.

[2] At the time of writing, the Assistant Deputy Coroner for Inner West London is completing an inquest into the 7 July 2005 bombings. As the Coroner has not reached any final conclusions on the attack, evidence

investigations into the bombings and information which became public during the conviction of five men arrested in 2004 whilst preparing for a separate bomb attack in the UK, with links to a number of the London bombers. Of the three reports, it is the ISC reports which provide the principal references for this case study, given their attention on intelligence analysis and the performance of the UK's intelligence community.[3]

Of the three case studies, the investigations into the London bombings resulted in the least amount of publicly released information of the three case studies presented in this thesis. The three reports run to a total of 184 pages, with some information redacted from the reports for security and legal reasons. There is limited primary evidence, such as analysts and officials' testimonies and declassified assessments, quoted within the ISC reports. Instead, instead these reports largely present the ISC's own conclusions, albeit based upon interviews with intelligence officials and reviews of classified material.[4] Consequently, this case study draws heavily on the ISC's interpretations of interviews and available evidence rather than primary evidence of analysts and officials. Nevertheless, these reports do provide insight into intelligence analysis, and the epistemological and methodological approaches used within intelligence agencies. The ISC drew upon evidence from heads of intelligence agencies, intelligence assessments on the "Islamist threat"[5], and their own reviews of "raw evidence" available to intelligence agencies and police.[6]

---

presented at the inquest is not included here. For transcripts of the Coroner's inquest, refer to http://7julyinquests.independent.gov.uk/hearing_transcripts/index.htm accessed 24 February 2011.

[3] The ISC did not distinguish between information and intelligence, thus the terms intelligence and information are used interchangeably in both ISC reports.

[4] *Ibid.*, p.3. Unlike the Australian Senate inquiry, the ISC had access to all classified information and assessments available to, and produced by, intelligence agencies.

[5] *Ibid.*, p.4.

[6] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, May 2009, The Stationery Office, p.4.

The agencies included in the ISC investigations were the Security Service (MI5)[7], Joint Terrorism Analysis Centre[8], Secret Intelligence Service (SIS) (MI6), Government Communications Headquarters (GCHQ), Cabinet Office, Joint Intelligence Committee (JIC, part of the Cabinet Office)[9], Foreign and Commonwealth Office, and Police (Special Branch and Specialist Operations).[10]

7.2 Ontology of Threat

The United Kingdom's intelligence agencies had been concerned with the potential threat from non-state actors long before the July 2005 attacks. The UK's intelligence community was acquainted with non-state threats, particularly with their experience with the Provisional Irish Republican Army (PIRA) during the 1970s-1990s. Whilst state-based threats did dominate UK intelligence efforts during the Cold War[11], agencies were well-aware of non-state threats. The ISC concluded that "…intelligence on Islamist terrorist

[7] The focus of the Security Service, more commonly known as MI5, is on threats within the United Kingdom, the SIS on external threats.

[8] In 2003, following the increased concern over the potential for major terrorist attacks, the UK Government established the Joint Terrorism Analysis Centre (JTAC), the British intelligence community's only single issue assessment body. Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005, London, The Stationery Office, May 2006 p.6. JTAC, part of the Secret Service, draws on additional analysts from across the intelligence community, including SIS, GCHQ, DIS, Foreign and Commonwealth Office, Home Office, and police. Cabinet Office, *National Intelligence Machinery*, 2nd Edition, The Stationary Office, September 2001, p.16.

[9] JIC "…is a part of the Cabinet Office, under the authority of the Secretary of the Cabinet. It is responsible for providing Ministers and senior officials with regular intelligence assessments on a range of issues of immediate and long-term importance to national interests, primarily in the fields of security, defence and foreign affairs. Cabinet Office, *National Intelligence Machinery*, 2nd Edition, The Stationary Office, September 2001, p.15. According to the ISC, "[b]oth the JIC and JTAC play an important role in analysing and assessing Islamist terrorism. ...The JIC produces strategic assessments of the threat from terrorism, aimed at presenting it in a wider context for senior decision and policy makers, including Ministers and officials". Intelligence and Security Committee, *Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, May 2006, p.25.

[10] The ISC explained the work of the Security Service, SIS and GCHQ in terms of support to the government's counter-terrorist strategy, CONTEST, and its four sub-elements: *Prevent* - draws on Agency work on the causes of radicalisation for extremists and terrorists; *Pursue* - involves Agency-led work on developing appropriate levels of capability to disrupt and bring to justice terrorist networks; *Protect* - encompasses the Agencies' work to provide protective security advice, from both physical and electronic attack; and *Prepare* - includes Agency input to risk assessments that underpin the resilience and response capabilities being developed. Intelligence and Security Committee, *Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.5.

[11] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors, House of Commons 898*, London, The Stationery Office, 2004, p.15.

networks (and particularly those planning attacks or with the capability to mount attacks on the UK) has been a JIC Priority Band 1 requirement for many years, well before the attacks in the US on 11 September 2001".[12] Nonetheless, the 11 September 2001 attacks did change agencies' perceptions of the nature and potential scale of non-state threats, resulting in a reallocation of effort. The Security Service's total operational effort against "the Islamist terrorist threat" rose from 23% over 2001/02 to 56% at the time of the 2005 attacks.[13] The significant shift in effort appeared to reflect a shift in threat-perception, rather than indicating a 33% increase in non-state threats.[14] Indeed, before the London attacks, the JIC had concluded that re-prioritisation of intelligence resources to counter-terrorism had reached the limits of what was possible without leaving the UK exposed to other threats.[15] So having reached the limits of reallocating resources, what did intelligence agencies understand about the nature and characteristics of non-state threats before July 2005?

The ISC identified a number of characteristics of the threat that were manifest in the London attacks and reviewed intelligence agencies' understanding and previous assessments on these specific characteristics. These characteristics included: the group was inspired by, or connected to, Al Qa'ida[16]; that the attacks were conducted by British

[12] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p. 33.
[13] *Ibid.*, p.33.
[14] The agency's efforts did result in disruptions of non-state threats between September 2001 and July 2005, including arrests and convictions of a number of Al Qa'ida and Al Qa'ida-inspired groups. Refer to Intelligence and Security Committee, Report into the London Terrorist Attacks on 7 July 2005, London, The Stationery Office, May 2006 p.41. The ISC reported that twelve attacks, all with the potential for mass-casualties, had been disrupted since 2000. Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.55.
[15] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.33.
[16] *Ibid.*, p.28.

citizens; the use of suicide as a tactic; and the targeting of London's transport network.[17] Before the July 2005, intelligence agencies were concerned with the potential threat from Al Qa'ida, affiliated groups and autonomous groups inspired by Al Qa'ida. A May 2005 JTAC report was quoted by the ISC:

> The UK threat picture is not currently dominated by one particular network or threat. The threat from Al Qaida [*sic*] (AQ) leadership directed plots has not gone away and events in Iraq are continuing to act as motivation and a focus of a range of terrorist related activity in the UK. However, many of our current concerns focus on the wide range and large number of extremist networks and individuals in the UK and individuals and groups that are inspired by but only loosely affiliated to AQ or are entirely autonomous.[18]

Following the September 2001 attacks in the US, intelligence agencies in the UK were focused on the threat both from Al Qa'ida and Al Qa'ida-affiliated networks. The ISC concluded that "[t]he complex nature of the threat from international terrorism, including from core Al Qaida [*sic*] at one end and unaffiliated groups and individuals at the other, had been assessed prior to July".[19] JTAC had developed a three-tiered model to help assess the degree of association between Al Qa'ida's leadership and individuals or networks and prioritise investigative efforts.[20] Applying this model retrospectively, the ISC discussed the shift in intelligence agencies understanding of the nature of the non-state threats developing in the UK. The ISC found that:

> In the aftermath of 9/11, Agency concerns were focused on Al Qaida [*sic*] networks, or 'Tier 1', and the possibility of attacks similar to those against the World Trade Center. This focus shifted, however, as more was learned and understood about the threat and its development within the UK. The group responsible for the Madrid attacks were assessed as belonging to 'Tier 3'. The

[17] *Ibid.*, p.25.
[18] *Ibid.*, p.23.
[19] *Ibid.*, p.27.
[20] 'Tier 1' described individuals or networks considered to have direct links with core Al Qaida; 'Tier 2', were individuals or networks assessed as more loosely affiliated with Al Qaida; and 'Tier 3', were applied to those assessed to not have any links to Al Qaida but might be inspired by Al Qa'ida's ideology. *Ibid.*, p.27.

> majority of extremists in the UK are also currently assessed as belonging to 'Tier 3'.[21]

Two months before the London bombings, JTAC had assessed that the majority of the non-state actors it was concerned with were those assessed as Tier 2 and Tier 3. That is, individuals or networks that were loosely affiliated with Al Qa'ida or altogether separate though sharing similar ideology.[22]

An additional characteristic was that of British citizens as threat actors. The ISC highlighted the development and changing perceptions of intelligence agencies in relation to potential attacks by British citizens within the UK. Between 2001 and 2005, and in the course of this, there was a marked change in agencies' perceptions of a "home-grown" threat. Assessments by JIC in 2002 suggested that attacks against the UK were more likely to come from foreign citizens entering the UK from abroad.[23] Subsequently, the ISC concluded that both perceptions of the threat and the non-state threat itself began to change. As evident from MI5 investigations, the non-state threat was changing even as intelligence agencies themselves attempted to understand what the threat was and what it would become.[24] These changes in the threat and perceptions of the threat were reflected within intelligence assessments. For example, in 2004, the Joint Intelligence Committee (JIC) "…judged that over the next five years the UK would continue to face a threat from 'home-grown' as well as foreign terrorists".[25] Nonetheless, the ISC concluded that "…the development of the home-grown threat and the radicalisation of British citizens were not fully understood or applied to strategic thinking".[26] In the aftermath of the London

[21] *Ibid.*, p.27.
[22] *Ibid.*, p.27.
[23] *Ibid.*, pp.25-26.
[24] This was evident in MI5 investigations and disruption of attacks within the UK. *Ibid.*, pp.25-26.
[25] *Ibid.*, p.25.
[26] *Ibid.*, p.30.

bombings, the ISC was informed that speed of radicalisation of individuals happened swifter than the agencies had anticipated, and without any external indicators that the radicalisation having occurred.[27]

The use of suicide as a tactic was described by the Committee as "…one of the most shocking aspects of the 7 July attacks".[28] Whether suicide bombings were anticipated by the intelligence agencies was, consequently, deliberately investigated by the ISC. The ISC did find that intelligence agencies had made assessments on the possibility of suicide attacks, but highlighted JIC's overall assessment that "…suicide attacks were not likely".[29] Consequently, the ISC concluded that suicide attacks within the UK on 7 July 2005 were "…clearly unexpected…".[30] The perception had been that "…extremists in the UK had been thought less likely to carry out suicide attacks because long-term indoctrination in the UK is more difficult than in countries with larger extremist communities and a more pervasive Islamic culture".[31] However, the ISC highlighted two previous attacks by British citizens outside the UK in which the attackers had attempted to use suicide.[32] The ISC's conclusion that the judgement that suicide attacks were not likely could have impacted upon the alertness of the authorities to the nature of the non-state threat, impacting authorities' ability to respond.[33]

The ISC concluded that, before July 2005, "…the intelligence and security community had identified and evaluated some elements of the possible sources and manifestations of the

[27] *Ibid.*, p.29.
[28] *Ibid.*, p.26.
[29] *Ibid.*, pp.26-27.
[30] *Ibid.*, p.28.
[31] *Ibid.*, p.28.
[32] The examples were the 22 December 2001 attempt by Richard Reid, a British national, to blow up a transatlantic flight with a shoe bomb and the 30 April 2003 attempted to conduct suicide attacks on a Tel Aviv bar by British citizens Omar Sharif and Asif Hanif. *Ibid.*, pp.26-27.
[33] *Ibid.*, p.29.

threat", including: the individuals were British citizens, living in the UK; the bombings were against "soft" targets (the London underground and bus network); and there was assessed to have been some connection with Al Qa'ida.[34] Nevertheless, the existence of a group planning the London attacks was not identified by intelligence agencies before the bombings. Neither were any of the four individuals involved in the attacks identified as threatening prior to 7 July. The Security Service was aware of the existence of two members of the group "…on the peripheries of other investigations".[35] Siddeque Khan and Shazad Tanweer had been observed meeting with Omar Khyam, who MI5 had under surveillance as part of Operation Crevice.[36] During surveillance, Khan and Tanweer were heard to discuss financial fraud and the success of the Madrid bombings, however as MI5 did not hear them discussing any bomb plot, the two were not identified as a top collection priority.[37] Once the Operation Crevice arrests had been made, MI5 reviewed over 4,000 contacts that those arrested had made in efforts to identify additional potentially threatening individuals, but neither Khan nor Tanweer was identified nor considered an immediate threat to life.[38] Indeed, it was only after the July attacks, and upon review of the Security Service's material, that Khan and Tanweer's identities were confirmed.[39] Consequently, the ISC concluded that "…none of the individuals involved in the 7 July group had been identified (that is, named and listed) as potential terrorist threats prior to July".[40] Based upon their investigations, and reviewing decisions made regarding collection priorities and intelligence targets, the ISC concluded that the decision to focus on other priorities rather than two individuals identified only in relation to possible fraud

[34] *Ibid.*, p.28.
[35] *Ibid.*, p.14.
[36] For details of Operation Crevice, refer to Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009.
[37] *Ibid.*, p.22.
[38] *Ibid.*, p.13.
[39] *Ibid.*, pp.15-39. Prior to this, Khan and Tanweer were defined simply as unidentified males (UDM).
[40] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.13.

was reasonable and understandable.[41]

The Home Office report, which attempted to deliver a factual account of the lead-up to the attacks, highlighted that the four bombers knew each other and had developed close relationships.[42] Hindering identification of the group, and discovery of their plans, was the group's "…meticulous planning with good security awareness including careful use of mobile phones and use of hire cars for sensitive activities associated with the planning of the attacks".[43] Additionally, the group appeared to have been self-financed and the materials used to make to bombs "…were all readily commercially available and not particularly expensive".[44] Even after the attacks, there remained uncertainty over aspects of the nature of the group, and in particular the nature of their links with Al Qa'ida.[45] This remained the situation almost four years after the attack, with solid evidence of the nature and links between Al Qa'ida and the four men remained elusive.[46] Consequently, even in 2009, the intelligence agencies could only assess it as *likely* that the bombers were directed in some way by overseas-based members of Al Qa'ida.[47]

In addition to the group's efforts to remain covert, the ISC consistently highlighted the scale of the collection and analytical challenge presented by potential non-state threat

[41] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, pp.42 & 54. Nonetheless, the Committee did conclude that more could have possibly been done to identify the London bombers, whilst at the same time acknowledging "…the sheer scale of the problem that our intelligence and security Agencies face and their comparatively small capacity to cover it". Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.16.
[42] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, pp.16 & 18.
[43] *Ibid.*, p.23.
[44] *Ibid.*, p.24.
[45] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.27.
[46] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.101.
[47] *Ibid.*, p.101.

actors as hindering accurate identification of threat actors.[48] The challenge here was two-fold: intelligence agencies have limits on their resources; and the sizeable number of already identified investigative priorities. The ISC emphasised the resource constraints that the intelligence community, particularly the Secret Service, operate within. The Secret Service's primary investigative targets within the UK had increased from 250 in late 2001 to 800 at the time of the July attacks.[49] The ISC was informed that Secret Service "[r]esources were fully consumed with the pursuit of existing leads and there was little capacity to look beyond to see where other threats might be developing".[50] For example, in 2004 it was assessed that MI5 could only provide reasonable coverage 6% of the overall identified threat.[51] If MI5 were required to provide comprehensive analysis on lower investigative priorities, the ISC suggested that, as a crude measure, the organisation would require a staff of several hundred thousand as opposed to the then strength of 3,500 personnel.[52] In a 2007 speech, the Head of MI5 argued that his agency was aware of around 2,000 potentially threatening individuals and groups either loosely aligned or simply inspired by Al Qa'ida within the UK. Additionally, there were perhaps the same numbers of similarly threatening individuals that MI5 remained unaware of.[53] The ISC made reference to the Director's speech, arguing that the figures were not scaremongering. Based on their investigations and understanding of the scale of the problem, the ISC similarly concluded that there were likely many more threatening individuals within the

---

[48] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.16.
[49] *Ibid.*, p.8.
[50] *Ibid.*, p.36. According to the Committee, "[a]n intensive operation, for example into imminent attack planning, can consume almost half of the Security Service's operational and investigative resources". *Ibid.*, p.7.
[51] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.41.
[52] *Ibid.*, p.42.
[53] Jonathan Evans, *MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust*, 5 November 2007, accessed at: www.cfr.org/publication/14789/mi5_director_generals_speech_on_intelligence_counterterrorism_and_trust_html on 9 May 2009.

UK of which MI5 remained unaware.[54]

As with US and Australian intelligence agencies, the principal concern of UK intelligence agencies' descriptions and assessments of threat was on the threat actors themselves. Even so, a review of the limited declassified assessments, and the ISC's own conclusions, brings to light a number of referents of threat. At the broadest level, the referent of threat was described as the United Kingdom, however more specific referents of threat are also evident from the investigations.[55] Immediately after the September 2001 attacks, government and iconic buildings within the UK were considered the primary target for Al Qa'ida-related or Al Qa'ida-inspired groups. However, from around April 2004, the intelligence community began to consider "soft" targets, such as transport networks and shopping centres, as the most likely for attacks. This change in thinking on the likely referent of threat appeared to be a direct result of the attacks on the rail network in Madrid, as well as information from ongoing investigations within the UK.[56] The London underground had been specifically identified as a potential target as early as April 2003.[57] Additionally, in May 2005 JTAC assessed that "…attacks on UK rail networks were high on the list of possible target options for terrorists and were likely to remain so".[58] Therefore, transport infrastructure, and the London Underground specifically, had been identified as a "possible" target for non-state threats, although no intelligence agency had information on the group planning the 7 July attacks. Nevertheless, whilst the kinds of targets were discussed largely in terms of buildings or infrastructure, the primary referent

[54] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.55.
[55] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, pp. 18-19. Only the highest level of *Critical* had a time attached, i.e. up to two weeks.
[56] *Ibid.*, p.26.
[57] *Ibid.*, p.26.
[58] *Ibid.*, p.26.

of threat was actually British citizens, as evident in the Director of MI5's emphasis that the highest investigative priorities being based on a threat to life.[59] Consequently, as "public safety" was MI5's top priority, investigative priorities were based upon individuals actually talking about conducting attacks.[60]

7.3 Epistemology of Threat

The United Kingdom's intelligence agencies appeared to assess threats on the basis of the dominant episteme, namely assessments of a group or individual's capability and intent. The use of Singer's model was apparent in JTAC's criteria for setting threat levels, which were, and are an attempt to quantify the threat to the UK.[61] JTAC used six levels of threat (*Negligible* to *Critical*), based on assessments of an individual or group's "capability" and "intent" to conduct an attack against a target. The criteria are founded on assessments on "available intelligence and recent events" in assessing capability and intent of a particular group or individual.[62] Under these criteria, the referent, or target, of threat was broadly defined as the United Kingdom.[63]

The approach to assessing threat was already familiar to the ISC, which had provided feedback on the criteria during an earlier investigation into the performance of the UK's Intelligence agencies following the 2002 Bali bombings.[64] However, the ISC did not use the opportunity to question the episteme underpinning the criteria, instead recommending the addition of another level to JTAC's existing model. In a fashion similar to the US and

[59] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.39.
[60] *Ibid.*, p.8.
[61] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p.17.
[62] *Ibid.*, pp. 18-19.
[63] *Ibid.*, pp. 18-19.
[64] Intelligence and Security Committee, *Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombings on Bali 12 October 2002*, London, The Stationery Office, December 2002, p.14.

Australian Committees investigating the performance of intelligence agencies, the ISC itself adopted the dominant episteme in describing threat and questions to the agencies. In describing Omar Khyam, who was arrested as part of Operation Crevice, the ISC mirrored agencies' model of threat arguing that "…intelligence showed he had both the intent and the capability to launch an attack".[65] Further, in considering information on Khan and Tanweer, the ISC asked MI5 "…whether there were any clues about their future intentions to conduct terrorist attacks".[66] Despite the primacy of Singer's model, the ISC's findings indicate that assessments of threat were not were not solely tied to the actor-based approach, despite the defined criteria being actor-based.

One of the notable assessments made by the JTAC was the lowering of the UK's threat level two months before the attacks. In May 2005 the threat level was decreased from *Severe (General)* to *Substantial*. *Severe General* was defined as: "…available intelligence and recent events indicate that terrorists have an established capability and current intent to mount an attack on the target or targets of this nature. It is assessed that an attack is a priority for the terrorists and is likely to be mounted".[67] *Substantial* was defined as: "…available intelligence and recent events indicate that terrorists have the capability to mount an attack on the target and that such an attack is within the group's current intent. It is assessed that an attack is likely to be a priority for the terrorists and might well be mounted".[68] Commenting on this downgrading, JTAC assessed that "…at present there is not a group with both the current intent and the capability to attack the UK".[69] JTAC argued that, as at May 2005, "…there was no firm intelligence of attack planning" as

[65] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, Cm7617, May 2009, p.21. Underlining as per ISC report.
[66] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.14.
[67] *Ibid.*, p.20.
[68] *Ibid.*, p.20.
[69] *Ibid.*, p.18.

"…the investigative leads that had previously been a cause for concern had been followed up and discounted".[70] Thus, JTAC concluded that in the absence of information of attacks being planned, the *Severe General* threat level could not be maintained.[71] Despite this assessment, JTAC argued that "[n]onetheless, the amount of continued and worrying activity, although it did not indicate current attack planning, was felt serious enough for a high level of threat to be maintained".[72] In reviewing this decision, the ISC concluded that even a downgrading to *Substantial* was "…perhaps still higher than the available intelligence warranted at the time according to the threat level definitions".[73] Thus, JTAC went beyond the defined actor-based criteria in setting threat levels, illustrating that agencies are willing to make assessments of threat beyond assessments of known groups' intentions and capabilities.

The downgrading of threat levels also highlights the limitations of an actor-based approach to assessing threat. The ISC acknowledged that "…threat levels represent a best estimate of what is happening" based on available information.[74] What the 7 July attacks demonstrated conclusively was that agencies are not necessarily able to identify all non-state threat actors, making assessments which rely on an understanding of a group or individual perforce limited. Noting that threat assessments had not been based upon knowledge of the group planning the London attacks, the ISC emphasised the limitations of the approach, drawing two conclusions: the first was the limits of knowledge; and the second was the visibility of the threat actors.[75]

[70] *Ibid.*, p.20.
[71] *Ibid.*, p.20.
[72] *Ibid.*, p.20.
[73] *Ibid.*, p.20.
[74] *Ibid.*, p.22.
[75] *Ibid.*, pp.30-32.

The ISC referred to an earlier Committee report, which had concluded that "…significant limitations in intelligence should be clearly stated and that assessments should make clear what is not known".[76] Articulation of the limitations was to ensure that those reading agency reports understood what confidence levels were being applied to the assessments. The proposal was questioned by the Home Secretary, who argued that "…to create a structure which stimulates certain forms of action on the basis of intelligence we do not have is a very, very difficult thing to do… it is better to use the intelligence we do have to inform our judgements insofar as we can".[77] There were no practical suggestions provided by the ISC on how the limits of existing knowledge might be assessed or how assessed levels of confidence would not simply reflect existing threat perceptions. Additionally, the Committee separately recommended that JTAC systematically include an assessment on the "level of visibility of the threat".[78] This recommendation highlighted the limits of applying the dominant episteme where threat actors are not identified or known.

Of all the case studies, it was the ISC reports that appeared to understand and articulate the limits of the dominant episteme most effectively. Whilst again not providing guidance on how to assess the visibility of threat actors, the ISC did advance the debate on epistemology of threat assessment. In the ISC's view, a combined assessment of the limits of intelligence and visibility of the threat would "…avoid the oversimplification of the UK threat picture and the potential for giving inappropriate reassurance about the threat".[79] This appeared particularly pertinent, given the previously discussed ISC and MI5 Director's comments on the possible numbers of unidentified non-state threat actors.

[76] *Ibid.*, p.31.
[77] *Ibid.*, p.22.
[78] *Ibid.*, p.43.
[79] *Ibid.*, p.43.

The ISC did identify limitations of the dominant episteme whilst attempting to ensure that these were factored into agencies' future assessments. However, the ISC did not deliberately consider alternative approaches to assessing threat beyond the actor-based model. Even so, there was evidence of alternative approaches to assessing threat beyond a reliance of knowledge of individual actors. Whilst the term threat environment was not evident within the investigation, a similar concept of a broader *threat picture* beyond specific actors was used by both the JTAC and the Committee. The JTAC used the idea of a *threat picture* beyond specific actors, arguing that "[t]he UK threat picture is not currently dominated by one particular network or threat".[80] The ISC also adopted this term in describing the broader context of threats, arguing that limitations of information and the visibility of the threat needed to be assessed.[81] The importance of *context* was apparent within assessments, with a number of factors used in understanding or assessing possible threats (both before and after the July bombings). Despite having no information on specific groups or individuals planning an attack, JTAC's acknowledged that concerns over "levels of activity" were factored into assessments of threat within the UK.[82] After the attack, a number of characteristics of the threat were being factored in to assessments of threat beyond specific actors. Radicalisation of individuals in the UK, particularly the potential speed at which this could occur, was one theme which emerged beyond reliance on observable behaviour of already identified threat actors. The development of *rich pictures* of local extremist behaviour was also highlighted as a development being pursued by intelligence and security agencies.[83]

[80] *Ibid.*, p.23.
[81] *Ibid.*, p.23.
[82] *Ibid.*, p.20.
[83] *Ibid.*, p.37.

7.4 Methodology of Threat Assessment

Intelligence agencies' analysis and assessments directly influenced decision-makers' understanding of the nature, characteristics and scale of non-state threats.[84] The assessed threat levels informed government and agencies' decisions about alert states and appropriate levels of security for the UK's critical national infrastructure.[85] In addition to accurate perception, the collection and analysis efforts of the intelligence agencies were perceived as fundamental to preventing attacks within the UK.[86] Intelligence agencies themselves are driven by assessments of threat.[87] Consequently, intelligence agencies' assessments also influence their own internal investigation priorities, resource allocations and actions. These perceptions of threat reflect intelligence agencies assessments of the most immediate threat to life.[88]

The ISC reports gave prominence to a number of themes of information and intelligence analysis, particularly the nature and volume of information and the limits of intelligence analysis. Whilst it highlighted the "overwhelming" volume of information received by agencies, it was the nature of information, and corresponding limitations, that the ISC deliberately explained for readers of their reports.[89] Quoting from other sources, or their own observations, the ISC described information as:

---

[84] *Ibid.*, p.25.
[85] Critical National Infrastructure (CNI) was defined as "…a term used within Government to describe the key sectors and services that support the economic, political and social life of the UK, the loss of which could be critical to the public and/or the Government". CNI included land transport, aviation and maritime sectors. *Ibid.*, p.17.
[86] *Ibid.*, pp.5-6.
[87] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.26.
[88] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.7.
[89] *Ibid.*, p.7.

- "sporadic and patchy, and even after analysis may still be at best inferential"[90];
- "fragmentary and difficult to interpret"[91];
- "some of it is misleading and much of it is irrelevant"[92]; and
- only giving "a partial picture".[93]

While MI5 did, as mentioned earlier, identify Mohammed Siddique Khan and Shazad Tanweer during Operation Crevice, there was no collected information which identified either of the two as having been involved in planning of a mass-casualty attack.[94] Neither the Home Office's nor the ISC's reports identified any collected information that identified preparation for the attacks, including information collected within the UK or provided by overseas agencies.[95] Instead, as previously noted, the ISC highlighted the limitations in collected information, emphasising that intelligence agencies cannot, and should not, collect every communication, and that agencies will always have gaps in their knowledge.[96] Even with information which became available following the attacks, the ISC concluded that they could not criticise the intelligence and security agencies based on the information available and their priorities before the attacks.[97]

Intelligence agencies assessed non-state threats based upon assessments of a network or

[90] Lord Butler, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors, House of Commons 898*, London, The Stationery Office, 2004, p.14, quoted in *Ibid.*, p.6.
[91] Dame Eliza Manningham-Buller, *Speech to the Dutch Security Service at the Ridderzaal, Binnenhof, The Hague, Netherlands, 1 September 2005*, quoted in *Ibid.*, p.6,
[92] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.44.
[93] *Ibid.*, p.5.
[94] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, pp.18-29.
[95] Refer to: Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.13; and Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, pp.72-73.
[96] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.7.
[97] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.54.

individual's capabilities and intentions. The application and importance of these assessments was evident in the Secret Service's criteria used to prioritise the agency's investigative efforts.[98] The three criteria against which individuals were assessed were: *essential*; *desirable*; and *other*.[99] It appears that the criteria were allocated to individuals based upon the agency's assessment of the person's capabilities and intentions.[100] Despite these parameters forming the basis of threat assessments and investigative priorities, there was actually very limited consideration of what assessments of intent and capability were drawn from. Many of the measures and indicators were apparent from the successful arrest and prosecution of individuals during Operation Crevice. Nonetheless, both the ISC and Home Office reports were particularly useful in identifying limits of measures, proxy-measures and indicators used for assessing capabilities and intentions.

There were no definitions of capability that appeared during investigations, however this parameter was understood within the context of the conduct of an attack.[101] There were a number of factors that can be identified as measures or proxy-measures for assessments of capability, with both quantitative and qualitative elements identified. As will now be examined, given that the group conducting the July bombings went undetected, it is apparent that a number of these factors were only apparent after the attack.

---

[98] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.8.

[99] *Ibid.*, p.8. Essential was defined as: an individual who is likely to be directly involved in, or have knowledge of, plans for terrorist activity, or an individual who may have knowledge of terrorist activity; Desirable was defined as: an individual who is associated with individuals who are directly involved in, or have knowledge of, plans for terrorist activity or who is raising money for terrorism or who is in jail and would be an essential target if at large; and Other was defined as: an individual who may be associated with individuals who are directly involved in, or have knowledge of, plans for terrorist activity.

[100] For example, when Omar Khyam was assessed to have "…both the intent and the capability to launch an attack" he was assessed as MI5's "top priority", and an "essential" intelligence target. Another (unidentified) individual was assessed as having "…both the intent and capability to launch an attack and posed a serious threat…" and subsequently defined as an "essential" target. Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, pp.21 & 29.

[101] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, pp.18-19.

People were fundamental measures of assessments of capability, as evident in investigations of individuals by agencies. The former Head of MI5, Dame Eliza Manningham-Buller, highlighted the incorrect belief held before 7 July 2005 "…that terrorist capability had been dented" by arrests of individuals during 2004.[102] Concern over "live bombs" further illustrated the centrality of people as a measure of capability.[103] In addition, weapons and explosives material were important measures of capability (as well as an indicator of intent), albeit not necessarily readily identifiable.[104] The Home Office concluded that the explosive devices "…were constructed with materials that are readily available commercially".[105] Where commercially available material was identified, it was taken as evidence of capability. The discovery of 600kg of ammonium nitrate stored in a London self-storage facility was taken as confirmation of Omar Khyam having both capability and intent and to conduct a mass-casualty attack.[106] Another unidentified individual was assessed as having "…both the intent and capability to launch an attack and posed a serious threat…" and was arrested "…whilst attempting to purchase automatic weapons and rocket-propelled grenades".[107] The London bombers also required knowledge to take commercially-available material and turn these into weapons, making knowledge an additional measure of capability. Unfortunately, as noted by the Home Office, this required limited expertise to turn the materials into bombs.[108] The cost of financing the attack was explored in some detail, with the conclusion that the cost of the attacks was

[102] Dame Eliza Manningham-Buller, oral evidence, 25 October 2005, in Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.20
[103] Head of MI5 quoted in Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.42.
[104] This is evident in that the group's bombs were not identified, or even known to exist, prior to the attacks.
[105] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.27.
[106] Discussed on page 113 of this thesis.
[107] *Ibid.*, p.29.
[108] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.27.

estimated at less than £8,000.[109] The Home Office's conclusion was that funds appeared to have come from legitimate sources: full-time employment; personal loans; and credit cards. This finding highlights the potential limitation in attempting to use funding as a proxy-measure of capability.[110]

As with capability, there appeared to be no deliberate definition of intent provided during the investigation, although it might be surmised as the desire of an individual or group to carry out an attack. There was considerably more discussion on the London bombers' intentions and the reasons that such intentions were not identified by intelligence and security agencies.[111] Additionally, discussion of individuals who were arrested, and successfully prosecuted, for planning mass-casualty attacks provided further insight into indicators used to assess intentions. Evidence of an individual's intent was a critical factor for MI5 to place an individual under surveillance, making identification of indicators of intent critical to investigative efforts.[112]

The importance of behaviour as an indicator of intent was identified by both the ISC and Home Office, which considered the group's outward behaviour as a basis for possible indicators of intentions. The ISC specifically asked MI5 "…whether there were any clues about their future intentions to conduct terrorist attacks".[113] The Home Office deliberately investigated the "[o]utward appearance of the bombers", concluding that "[t]he behaviour

[109] Home Office, Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.23.
[110] *Ibid.*, p.27.
[111] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, pp.14, 36 & 39; and Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, pp.44, 48 & 74.
[112] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.44.
[113] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p.14.

of the bombers in the run up to 7 July appeared generally normal to those around them, with the exception of Lindsay".[114] Despite Lindsay's behaviour being erratic and possibly indicating criminality, it did not arouse suspicions of "terrorist intentions".[115] Khan and Tanweer's association with people already under investigation by MI5 was considered, but only in hindsight, as a potential indicator of hostile intentions.[116] Within the context of radicalisation, associations also appeared to present a potential indicator of the development of hostile intent. Additionally, visits to Pakistan were considered a potential indicator of intent, with the ISC concluding that greater coverage in Pakistan "…might have alerted the Agencies to the intentions of the 7 July group".[117] Nonetheless, the Home Office highlighted that the men's visits to Pakistan would not necessarily have appeared out of the ordinary, particularly when there were almost 400,000 visits by UK residents to Pakistan in 2004, with an average stay of 41 days.[118] Therefore, the travel alone would not necessarily stand out to intelligence agencies as an indicator of intent.

A critical indicator of intentions, which helped intelligence agencies determine investigative priorities, was the words spoken by individuals. The reliance on surveillance and eavesdropping during Operation Crevice and Operation Rhyme emphasised the importance on words as indicators of intentions.[119] MI5 surveillance during Operation Rhyme consisted of six weeks of 24 hour coverage involving, 15 surveillance teams, 20

[114] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.24.
[115] *Ibid.*, p.26.
[116] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p.36.
[117] *Ibid.*, p.39.
[118] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.21.
[119] Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.12. Operation Rhyme was an MI5 operation against a group planning a series of coordinated, mass-casualty attacks in the UK. There was an allegation that the group was planning to put radioactive material in explosives to make "dirty bombs". Eight individuals arrested in connection with the operation were subsequently convicted of terrorist offences. *Ibid.*, p.12.

CCTV cameras with 8,000 hours of surveillance product, 25,000 hours devoted to monitoring and transcription and analysis of seized hard drives with 2.5 terabytes of data.[120] Against this, as Khan and Tanweer were not identified talking about planning to conduct an attack, there appeared to be no intention to conduct an attack.[121] It appears, therefore, that the group's operational security, including "careful use of mobile phones", and an indication that Khan was concerned about being under surveillance, hindered efforts at using words as indicators of intent.[122]

Dissimilar to the two previous case studies, there was an absence of a *post-hoc* application of the dominant episteme and methodology during the investigation. This might have been due to the limited release of primary evidence from analysts and officials. Additionally, this could have reflected the fact that the particular group that conducted the attacks no longer existed once the bombings had been conducted. Alternatively, at least one official, the Head of MI5, argued that even a review of material after-the-event emphasised that there was no information that indicated Khan or Tanweer's "…intention to mount terrorist attacks in the United Kingdom".[123] That is not to suggest that officials or the Committee did not shift perceptions after the attacks. The ISC and officials did re-assess non-state threats based upon the nature and characteristics apparent in the attacks, but at a generic level, as indicators of the kinds of issues that needed to be given greater attention. The attacks reinforced the scale of the collection and analytical problem, with efforts aimed at

[120] *Ibid.*, p.12.
[121] *Ibid.*, p.48.
[122] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.24. A November 2004 home video of Khan saying goodbye to his daughter was only identified after the London attacks and appeared to relate to an earlier trip to Pakistan, where he did not expect to return from. See Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.48.
[123] Oral evidence from the Head of MI5, 14 June 2007 quoted in *Ibid*., p.54.

increased "coverage" of non-state threats within the UK and abroad.[124] Additionally, the speed of radicalisation of those involved in the attack was also taken as a priority for intelligence and security agencies to better understand.[125] Reviews of old operations were also emphasised as a possible approach to uncovering new leads, and using the benefit of hindsight to see old material in a new context.[126] Thus, rather than a *post-hoc* application of intent and capability, intelligence agencies and the ISC appeared to identify more generic trends about potential future non-state threats as a basis for more proactive approaches to intelligence collection and analysis.

7.5 A More Comprehensive Model of Threat

The 2005 London bombings provide an insight into how elements of a more comprehensive model of threat were being considered in intelligence assessments of threat, albeit not defined within the threat assessment criteria. The London underground had been specifically identified as a potential target of an attack, irrespective of the absence of information on a specific threat actor planning such an attack. Consequently, whilst citizens would be considered the target, the fact that public transport had been specifically considered highlighted the importance of defining the possible referent of a threat. The result was that, whilst the specific attack came as a surprise, unlike the Bali bombings and attacks in the United States, that the London underground was selected as a target was not a surprise. In terms of the environmental factor, namely concern over non-state threat actors inspired-by or part of Al Qa'ida, this had reportedly been a priority of British

[124] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p.34
[125] *Ibid.*, p.35.
[126] Oral evidence from the Head of MI5, 14 June 2007 quoted in Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, London, The Stationary Office, May 2009, p.46.

intelligence agencies before the attacks.[127] Additionally, intelligence agencies reportedly kept threat levels at a level higher than the intent-capability criteria suggested based on the amount of concerning activity. The result was that despite having no information on specific groups planning an attack, the assessed level of threat was closer to the reality of the situation than had it been solely determined on identified *intentions* or *capabilities*. The issue of visibility of the threat was subsequently recommended as being formally captured in assessments. Interestingly, factors evident in a *situational* approach, namely radicalisation of individuals, were reportedly considered by intelligence analysts (though again not formally captured in the concept of threat employed). The conclusion was that radicalisation of individuals required long-term indoctrination, which was thought to be less likely in the UK than in other states. The speed and nature of radicalisation was then taken as a priority for intelligence and security agencies, highlighting the potential focus on a *pre*-intentions and capabilities *situational* approach to the emergence of non-state threat actors. Thus, whilst some factors beyond the conventional threat parameters were considered, a number of conclusions about these proved to be incorrect highlighting that even where identified assessments will not necessarily reflect reality. The importance of these factors does however highlight their potential importance in arriving at a more comprehensive model of threat.

[127] Reallocation of intelligence resources following the bombings does, however, indicate a further reprioritisation of intelligence efforts.

Chapter 8:

A critique of Singer's model in practice

> There has been only modest emphasis internally on looking at failures—and even less on examining successes—with an eye to drawing lessons for self-improvement…
>
> Warren Fishbein and Gregory Treverton[1]

Singer's model requires ideal conditions for it to work. It could be argued that the Cold War provided these conditions, with neatly defined state-based threats being the primary focus of intelligence analysis within the United States, United Kingdom and Australia. Where the focus was on the threat of nuclear warfare between states, the assumption could be made that understanding threat was simply a matter of looking at a state's military forces and political hierarchy to come to a conclusion about capability and intent. Consequently, Singer's model has very little to say about the complexity of the existing security environment apparent in examination of the incidents discussed in the previous three chapters.

As demonstrated in the case studies, recent mass-casualty attacks by non-state actors do not present the ideal conditions as envisaged by the use of the conventional model. These attacks were not achieved by the massing of armies, movement of large weapons, or a myriad of other indicators or measures of state-based threats. Nor were individuals involved in these attacks linked to political hierarchies, military organisations, state bureaucracies or reactive to traditional approaches to modifying states' behaviour. Instead, the threat was from relatively small, spread out, amorphous organisations killing

[1] Warren Fishbein and Gregory Treverton, *Rethinking "Alternative Analysis" to Address Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.2, October 2004.

a lot of people by available means.[2] These incidents highlight that such groups, as difficult as they are to identify and understand, can cause the deaths of thousands of citizens, even with relatively limited resources at their disposal. Examination of these three incidents helped to illuminate similar and distinct aspects of the analytical challenge of non-state threats, with an eye on moving debate beyond an uncritical acceptance of the conventional model.

8.1 Comparison and contrast of incidents

The three attacks described in the case studies were shocking, traumatic events for citizens and governments, collectively resulting in the deaths of over 3,000 people over a four-year period. These incidents amplify the increasingly complex security environment within which non-state actors and states function and elevate the requirement to accurately identify and assess threats at the individual level. The investigations and inquiries begun in the months following each attack resulted in the public release of otherwise classified material provides an insight into the practical application of the intent-capability model to assessing non-state threats. Whilst these attacks were all conducted by non-state actors, they were distinct in terms of the characteristics of the groups conducting them and the size, location, scale and nature of the attacks themselves. This, of itself, suggests broad limitations of the conventional approach even when applied to dissimilar non-state threats.

The September 2001 attacks were conducted by Al Qa'ida, a group already identified by US intelligence agencies as being responsible for previous attacks against US citizens

[2] Brian Jackson, Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda, *Studies in Conflict & Terrorism*, Vol.29, 2006, pp.241–262, p.242.

outside the United States. Nineteen individuals, most not known to be associated with Al Qa'ida, carried out the attacks using US resources to kill nearly 3,000 people, primarily US citizens. Using suicide as a tactic, the group achieved both a scale and style of attack which had never before been achieved either within, or for that matter outside of, the United States. The attacks underscored the difficulty of dealing with foreign non-state threat actors within the United States.

For Australian intelligence agencies, the Bali bombings represented an attack by a foreign-based non-state actor against Australian citizens overseas. Members of Jemaah Islamiyah, the group responsible for the bombings, had deliberately hidden the organisation's existence, and so intelligence analysts could not quite come to terms with the nature or membership of the group before the attacks. The Bali bombings were of a style and scale never before achieved in Southeast Asia, and were in contrast to the previous behaviour of JI.

Unlike foreign-based groups involved in the New York-Washington and Bali attacks, the London bombings were carried out by British citizens against fellow-British citizens within the United Kingdom. Just four individuals appear to have planned, funded and conducted the largest attacks in London since World War Two. Whilst two of the four individuals had been identified by the Secret Service, this had been only in the context of potential low-level fraud. Consequently, the group and the plot remained undetected until the actual bombings. These points are displayed in Table 2 to assist in comparison of the incidents.

Threat Actor	Location of attack	Nature of attack	Referent
Foreign-based group.[3]	New York and Washington, United States.	Attack on prominent buildings using hijacked planes as weapons.	Primarily US citizens.
Foreign-based group.[4]	Bali, Indonesia.	Bombing of Bali tourist district using vehicle-borne bomb and a backpack bomb.	202 people killed, including 88 Australian citizens.[5]
Locally-based group.[6]	London, United Kingdom.	Bombing of London transport infrastructure using four backpack bombs.	Primarily British citizens.

Table 2: Nature of three incidents by Threat Actor, Location, Nature and Referent.

Intelligence agencies' understanding of the nature and characteristics of the groups before each attack demonstrates the analytic challenge presented by non-state actors. Prior to the September 2001 attacks, US intelligence priorities had been on state-based rather than non-state threats.[7] Similarly, the argument was made that it took the September 2001 attacks in the United States and the October 2002 bombings in Bali for Australian intelligence agencies to recognise non-state threats to security.[8] This contrasted with the UK's intelligence agencies, which were focussed on "Islamic terrorist networks" well before the September 2001 attacks.[9] Nevertheless, regardless of priorities assigned to non-state threats prior to each attack, each incident came as a surprise to intelligence agencies. Indeed, these attacks each resulted in significant reallocation of resources within the US, Australia and UK indicated a certain reactiveness to these threat

[3] Nineteen individuals from Saudi Arabia, UAE, Egypt and Lebanon identified as members of Al Qa'ida.
[4] Unidentified number of Indonesian citizens linked to Jemaah Islamiyah.
[5] There were 38 Indonesian citizens killed in the attack, with the remaining 164 people being tourists from over 20 different countries.
[6] Four British citizens likely linked to Al Qa'ida.
[7] Refer to Chapter 5:2 *Ontology of Threat*.
[8] David Wright-Neville, former ONA analyst, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 November 2003, pp.259-260.
[9] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p. 33.

actors, irrespective of the stated priorities prior to the attacks.

Evident in each investigation, the respective intelligence agencies were unable to accurately identify the nature and characteristics of the groups responsible for the attacks. The inability of US and Australian analysts to identify the boundaries of Al Qa'ida and JI respectively was a notable shortcoming, although whether or not such delineations are achievable is debatable. In each case, intelligence agencies perceived groups different to what they actually were. This was particularly apparent in the FBI's perception that "…al-Qa'ida had limited capacity to operate in the United States and any presence here was under surveillance".[10] This inability to define the organisation meant that US intelligence analysts were assessing Al Qa'ida as they understood it, but not as it actually was. Whether this problem was resolved after the September 2001 attacks remains a matter of ongoing debate. Writing in 2010, on the ninth anniversary of the September 2001 attacks, George Friedman argued that the US intelligence community had failed for a decade "…to understand what al Qaeda was and wasn't".[11] According to Friedman, "[t]he greatest failure of American intelligence was not the lack of a clear warning about 9/11 but the lack, on Sept. 12, of a clear picture of al Qaeda's global structure, capabilities, weaknesses and intentions".[12]

The inability of Australian intelligence agencies to define and understand JI was evident during the Senate inquiry. In the run-up to the bombings, agencies had very limited

[10] Former National Security Advisor, Sandy Berger, quoted in Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.26.
[11] George Friedman, *9/11 and the 9-Year War*, 8 September 2010, accessed on 12 September at www.stratfor.com/
[12] *Ibid.*

understanding or JI membership, relationships and cell structures.[13] Between the discovery of JI and the Bali bombings, intelligence agencies did not establish an understanding of the membership, structure, plans or even the way the JI organised itself.[14] Consequently, whilst analysts were "…trying to get a better picture of how Jemaah Islamiyah was structured and would operate…", this proved unachievable.[15]

In May 2005, the Joint Terrorism Analysis Centre had downgraded the assessed level of threat within the UK, assessing that there was no group with an intent or capability to conduct a mass-casualty attack.[16] In fact, there were at least two groups preparing attacks: the 7 July attacks; and those involved in the 21 July attempted bombings[17]. Neither of these groups were identified before the attacks and attempted attacks some two months after JTAC's assessment.

In the case of Al Qa'ida and JI, the transnational nature of these groups increased the difficulty for intelligence agencies in a number of ways. Because neither of these groups was confined to any one location, identifying, tracking and monitoring individuals as well as confirming associations and planning proved extremely difficult. Further, the transnational nature of both organisations also presented intelligence agencies with the problem of a multitude of potential targets that could be attacked.[18]

---

[13] Frank Lewincamp, Director DIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.55; and Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.161.

[14] William O'Malley, Assistant Director-General, Southeast Asia Branch, ONA, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.126.

[15] *Ibid.*, p.126.

[16] Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006, p.18.

[17] Whilst the devices failed to detonate, the chemicals used were viable to be used to make bombs. According to testimony given at the court case, it would not have been predictable before hand to know whether or not the bombs would detonate. Testimony quoted in http://itn.co.uk/3967b7a45c8a1847f5ba6d060069a0ec.html accessed 9 July 2009.

[18] Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28

A noteworthy aspect of each attack was that groups and individuals behaved differently to how they were assessed. These assessments were based largely upon the group's previous behaviour, as well as the observed behaviour of individuals linked to these organisations. Consequently, shifts in behaviour proved problematic for achieving accurate assessments of the threat, meaning that any previous post-hoc assessments of intent and capability would not have provided insight into future threat. In the case of the Bali bombings, JI behaved differently to the way they had in the past. Just one month prior to the attacks, DIO pointed to a lack of attacks against Western interest and a pattern of attacks against Southeast Asian targets.[19] Shortly after the bombings, the same agency noted that "[t]he Bali bombings demonstrated an intent and capability to cause high civilian casualties not seen before in South-East Asia".[20] Thus, analysis of previous JI attacks would not have been a useful basis for assessments of their future behaviour.

Prior to September 2001, there had been attacks attempted within the US, however these had been disrupted or failed to deliver the envisaged mass-casualties.[21] Consequently, the Committee concluded that "…the assumption prevailed in the US Government that attacks of the magnitude of September 11 could not happen here".[22] Thus, the scale and nature of the attacks came as a surprise to the US intelligence community, albeit not the identity of the organisation responsible. Although the US intelligence community had been concerned about an attack, the assessment, and the analysis provided to

---

May 2004, p.460.

[19] *Ibid.*, p.5.

[20] Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on notice 20 June 2003, p.5.

[21] The 1993 World Trade Centre bombing had not achieved the collapse of the building as was reportedly the aim.

[22] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.xix.

government, was that this would most likely occur overseas.[23] In the context of the London bombings, whilst the group planning the attacks had not been identified, it was apparent that intelligence agencies had not expected British nationals to be involved in suicide attacks in the UK.[24]

The disproportionate nature of mass-killing power is also apparent in each incident. That small numbers of individuals could kill tens, hundreds and thousands of people in attacks makes identifying and accurately assessing threat a critical task for intelligence agencies. This is particularly so given Governments' repeated commitments to protecting their citizens as their highest priority. In each of the three attacks, once the identities of those involved had been confirmed, it was established that some individuals *had* been known to agencies. Nevertheless, none of the individuals involved in any of the incidents had been identified as being part of a larger group planning the attacks. The inability of intelligence agencies to link individuals to threatening groups provides at least a partial explanation for the gap between what these groups were understood to be and what they actually were.

As discussed, before the London bombings, two individuals (later identified as being involved in the attacks) had been caught on MI5 surveillance on the periphery of another MI5 investigation. However, this was not within the context of preparing a mass-casualty attack. Even some four years after the attacks, the UK's intelligence agencies remained uncertain over the nature of the group's links with Al Qa'ida. The investigation into the attacks in the US revealed that sixteen of the nineteen hijackers were not known to be

[23] Samuel Berger, written testimony, Second Public Hearing 19 September 2002, p.6, available at: http://www.fas.org/irp/congress/2002_hr/091902berger.pdf
[24] *Ibid.*, p.28.

associated with Al Qa'ida[25], and appeared to have been deliberately chosen for this reason.[26] The locations or activities of the remaining three individuals associated with Al Qa'ida were not identified by intelligence agencies. Perhaps indicative of the difficulty in linking individuals with threatening groups is the example of Zacchius Moussaui, who the FBI originally had difficulty connecting to a listed terrorist group, even though they had him in custody.[27] The combined Indonesian Police (POLRI) and Australian Federal Police (AFP) investigation revealed the identities of those involved in planning and conducting the bombings in Bali, with only some of those identified known to intelligence agencies.[28] Additionally, the difficulty in dealing with threats at the individual level was apparent in Australian agencies' acknowledged inability to track the movement of already-identified JI members across Southeast Asia.[29]

According to Treverton, a challenge for analysis about state-based threats during the Cold War was that of too little information. On the other hand, current non-state threats present analysts with the difficulty of too much information.[30] Technology has enabled the collection of vast quantities of information without a corresponding enabling of analysts to analyse this collected data. As noted in the findings of the US, Australian and UK investigations, which noted that before the attacks, the volume of collected information was proving overwhelming for analysts to deal with.[31] Moreover, despite the

[25] Eleanor Hill, Joint Inquiry Staff, *The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001*, September 20, 2002, p.4, at: http://www.fas.org/irp/congress/2002_hr/092002hill.pdf
[26] *Ibid.*, p.4.
[27] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.315-324.
[28] Refer to testimony of William O'Malley, Assistant Director-General, Southeast Asia Branch, ONA, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.126.
[29] *Ibid.*, p.124.
[30] Gregory Treverton, *Intelligence for an Age of Terror*, Cambridge University Press, New York, 2009, Table 1.1, p.2.
[31] Samuel Berger, testimony to Joint Inquiry into Intelligence Community Activities before and after the

overwhelming volume of information being collected, no agency identified any specific information which established the timing or location of any of the attacks, nor the existence of cells and individuals planning them. This lack of information is worth considering, given that Singer's model assumes that decision-makers and analysts have access to such information. The Australian Committee actually discussed this lack of information specifically, noting that whilst analysts do pursue specific information, they are almost invariably settling for less, yet are still required to make sound judgments.[32] This inability to collect specific and insightful information on each of these groups can be linked to the operational security measures taken by those involved in the attacks. Indicators of intentions, both physical and verbal, went largely unidentified by the intelligence community as a consequence of deliberate efforts by the hijackers to avoid detection. Operational security relating to both communication and observable behaviour appeared to be critical in the preparations and planning for each of the attacks, hindering intelligence agencies' efforts to identify these, even where they knew of broader groups' existence. In none of these cases did these groups' communications stand out, a point made during each of the investigations.

Those within Al Qa'ida "…were very concerned with operational security, including relying on face-to-face meetings and speaking in code to disguise details of operations".[33] This was also reflected in the hijackers' careful use of telecommunications prior to the attacks.[34] Similarly, their behaviour aroused no suspicions when they were in

---

Terrorist Attacks of September 11, 2001, 19 September 2002; Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.18; and Intelligence and Security Committee, *Report into the London Terrorist Attacks on 7 July 2005*, London, The Stationery Office, May 2006 p.7.

[32] Senator Hutchins (Committee Chair), Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.452.

[33] Eleanor Hill, *Joint Inquiry Staff Statement, Part I*, September 18, 2002, p.13 at: http://www.fas.org/irp/congress/2002_hr/091802hill.pdf

[34] *Ibid*., p.13.

the US[35], dressing and behaving in a manner to avoid attention.[36] JI's careful use of telephone and internet was noted[37], as was their use of code and cover terms.[38] Furthermore, their behaviour led to the observation that members of JI "…look like ordinary people going about their everyday business".[39] In the UK, the London bombers operational security measures included the "careful use of mobile phones".[40] The investigation of the men's behaviour led to the conclusion that their behaviour prior to the attacks did not arouse suspicion, with only one man's behaviour suggesting possible low-level criminality, but not preparations for mass murder.[41]

This issue of operational security could be viewed as being solely indicative of factors *internal* to these groups, however it should be understood in the broader context as also reflecting factors *external* to the group. That individuals' behaviour did not arouse suspicion does not simply reflect the individual but the broader social environment within which they operated. Again, as with threat, *abnormal* or *unusual* behaviour is that which is in contrast to the broader societal group. That many of these individuals were able to live and prepare attacks within cities without drawing attention also speaks to the nature of the social surroundings, within which people are able to maintain a level of anonymity.[42] Additionally, the careful use of communications technology is reflective of

---

[35] Robert Mueller, *Statement for the Record, FBI Director Robert S. Mueller III, Joint Intelligence Committee Inquiry*, Closed Hearing, 25 Sep 2002, p.2, declassified statement at: http://www.fas.org/irp/congress/2002_hr/092602mueller.pdf

[36] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, p.168

[37] *Ibid.*, p.105.

[38] Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353.

[39] Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353.

[40] Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006, p.24.

[41] *Ibid*, p.24.

[42] This point of anonymity within urban settings is highlighted by Zimbardo. Philip Zimbardo, *The Lucifer Effect*, Random House, New York, 2007, p.304.

a societal context within which the use of communications and the expansion of communicated information are repeatedly described in terms of an 'information revolution'. Consequently, society's adoption and prolific use of information technology, by its very ubiquity, helps disguise individual communication irrespective of the small group's operational security. As a result, it is not simply a matter of intelligence analysts overcoming a group's internal operational security but understanding the way in which the broader physical and communications environment actually assists in enhancing anonymity.

8.2 Limitations of Singer's model in practice

Examination of investigations into these incidents indicate that intelligence agencies, officials and analysts do use Singer's concept of threat in practice; assessing and prioritising non-state threats primarily based upon assessments of organisations or individuals' capabilities and intentions. This analytic and perceptual homogeneity is worth noting, given that a consistent refrain within the intelligence literature is the requirement for new and different thinking in intelligence analysis.[43] Thus, whilst there appears to be a perceived benefit in analysts employing different analytic techniques, as evident from the investigations this does not, at least at the time of these attacks, appear to occur in practice.

[43] For example, refer to: Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005, p.5; Philip Flood, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004, p.36; John Scarlett (then JIC Chairman), *Annual Review by the JIC Chairman: 2003–2004*, quoted in Intelligence and Security Committee, *Annual Report 2004–2005*, The Stationery Office, 2005, p.19; Mike McConnell, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58, p.53; Arthur Hulnick, What's Wrong with the Intelligence Cycle, *Intelligence and National Security*, Vol.21, No.6, December 2006, pp.959-979, p.94; Frederick Hitz and Brian Weiss, Helping the CIA and FBI Connect the Dots in the War on Terror, *International Journal of Intelligence and Counter Intelligence*, Vol.17, 2004, pp.1-41, p.29; and Bruce Berkowitz, The New Protracted Conflict: Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, Pages 289-300, p.292.

The release of threat assessment criteria during the Australian and British investigations illustrated the strict adherence to the model described by Singer and revealed the lack of development of the model over the previous decades.[44] Similarly, analysis of the concepts of threat described during the US inquiry emphasised the ongoing use of the model.[45] Nevertheless, whilst concepts of threat were reliant on assessments on the threat actor, in none of the incidents was the identification and understanding of the threat actor achieved. Instead, in each incident, the measures, proxy-measures and indicators of these groups' capabilities and intentions remained ambiguous up until the actual attacks. The superficially benign nature of killing power used in the September 2001 attacks potentially hindered accurate identification of both the actor and their capabilities. In the case of the Bali bombings, the availability of explosives within an area the size of Southeast Asia limited agencies' ability to confirm whether JI actually had access to these. Finally, the four men in the UK built their own bombs out of readily available materials, and reportedly did so without raising suspicions. Awareness of operational security hindered the identification of hostile words or behaviour, undermining efforts at identifying indicators of intent. As evident in each of the incidents, unambiguous measures, proxy-measure and indicators of non-state actors' capabilities and intentions to conduct mass-casualty attacks were not identified and were, therefore, not a given. These incidents highlight that *both* intentions and capabilities have significant and, potentially, unavoidable limitations and weaknesses in assessing non-state actors. Arguably, one of the most revealing aspects in this respect is that the conventional approach was applied across three very different non-state attacks with the same result. In each incident the attacks came as a surprise with intelligence agencies unable to

[44] Refer to Chapter 6, Section 2, *Epistemology of Threat*, and Chapter 7, Section 2, *Epistemology of Threat* for Australian and UK threat assessment criteria.
[45] Refer to Chapter 5.3 *Epistemology of Threat* for a discussion of the US reliance on the conventional approach.

accurately identify the threat actors involved.

Whilst officials and analysts did not appear to deliberately identify limitations of the conventional approach, the actions of analysts in both Australia and the United Kingdom indicate an implicit acknowledgement that threat was more than just assessments of intentions and capabilities.[46] Investigations into the London and Bali bombings indicated that analysts in both the UK and Australia actually did go beyond the conventional approach. Analysts drew upon factors external to specific groups in setting threat levels above what would have been warranted if relying solely upon assessments of known groups' capabilities and intentions. In assessing the threat level for Indonesia, Australian analysts went beyond their own defined criteria, factoring in a number of issues *external* to assessments of threatening organisations within Indonesia. These factors included consideration of: the attacks of September 2001 in the US; potential for US attacks on Al Qa'ida in Afghanistan[47]; publicity within Indonesia of attacks against mosques and Islamic institutions in Australia[48]; Osama bin Ladin's public reference to 'crusader Australian forces'; and a recurring elevation of Australia's profile as a US ally in actions against Al Qa'ida.[49] In addition, agencies also made assessments on JI based on factors external to the organisation, reflecting the "…the near impossibility of extracting information about (let alone from) tightly knit, cell-based groups of carefully recruited militants".[50] Thus, assessments of JI's capabilities and intentions were based upon both the limited information that agencies could gain on JI as well as judgements about: how these types of groups operated; the phenomenon of bin-Ladin 'global jihad'; availability

[46] Discussed in detail on pp.196-197 and p.224 of this thesis.
[47] Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, pp.3-4.
[48] *Ibid.*, p.3.
[49] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.28.
[50] *Ibid.*, p.105.

of weapons and explosives across the region; porous borders; and limited domestic constraints on non-state threats.[51] Despite the dominant episteme of threat being based upon an actor's assessed intentions and capabilities, Australian intelligence agencies did appear to factor in events and influences external to JI, albeit without formally defining these.

In downgrading the assessed threat level for the UK, JTAC argued that "[n]onetheless, the amount of continued and worrying activity, although it did not indicate current attack planning, was felt serious enough for a high level of threat to be maintained".[52] In reviewing this decision, the ISC concluded that even a downgrading to *Substantial* was "…perhaps still higher than the available intelligence warranted at the time according to the threat level definitions".[53] Thus, the intelligence agency went *beyond* its own actor-based criteria in setting the threat levels, illustrating that agencies are willing to make assessments of threat beyond assessments of known groups' intentions and capabilities. Therefore, the actions of analysts in the UK and Australia indicate a tacit acknowledgement that threat is more than the assessment of intent and capability.

Beyond officials and analysts, each Committee adopted the conventional model of threat both for describing non-state threats and as a basis for assessing agencies' performance. Indeed, the UK's ISC had already evaluated the existing approach, recommending additional levels to the model, without challenging the dual-parameter approach to assessment.[54] Thus, during each investigation, the opportunity to deliberately critique the conventional approach was missed. Whilst alternative approaches for assessing non-state

[51] *Ibid.*, p.105.
[52] *Ibid.*, p.20.
[53] *Ibid.*, p.20.
[54] Intelligence and Security Committee, *Inquiry into Intelligence, Assessments and Advice prior to the Terrorist Bombings on Bali 12 October 2002*, London, The Stationery Office, December 2002, p.14.

threats, namely those of vulnerability and environmental methodologies, were touched upon during the each of the investigations, these appearances were fleeting. Consequently, neither was given deep consideration as an *alternative* to the dominant model. Indeed, there was no evidence of alternatives to the conventional approach entertained during any of the investigations. Nevertheless, each Committee did indirectly shed light on different limitations of Singer's approach.

Reflecting the diverse nature of the attacks which they were looking at, each investigation provides faceted insights into the limitations of Singer's model, enabling a broad critique of the approach to assessing non-state threats. What each of the Committees' final reports reveal is that threat is a more complex concept than Singer's model suggests. This was particularly apparent in Committees' assessments of the performances of intelligence communities in the United States and Australia. In reviewing intelligence assessments before the September 2001 attacks, the Joint Committee concluded that the US intelligence community "…repeatedly warned that al-Qa'ida had both the capability and the intention" to threaten Americans.[55] Similarly, the Australian Committee concluded that agencies had warned that "Indonesia-based terrorists had the intention and capability to mount attacks against Western interests, and that Australian interests could not be regarded as exempt from such attacks".[56] Nevertheless, in both inquiries it was apparent that such assessments were not enough and did not capture the broader concept of threat. The Joint Committee concluded that intelligence agencies had failed to understand the collective significance of information that they had already collected.[57] Additionally, the Committee noted the

[55] *Ibid.*, p.242.
[56] Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xiv.
[57] Joint Inquiry into Intelligence Community Activities before and after the Terrorist Attacks of September 11, 2001, *Report of the US Senate Select Committee on Intelligence and the US House Permanent Select Committee on Intelligence*, 107th Congress, 2nd Session, December 2002, pp.69-70.

community's "slow response" to the transnational threat[58], finding that the US intelligence community's analytic efforts to understand the scope and nature of Al Qa'ida were inadequate[59]. The Australian Committee concluded that intelligence agencies should have focussed specific assessments on Bali because of the large numbers of Australians and Westerners there, the presence of hotels, nightclubs and an acknowledged desire by non-state actors to attack 'soft targets'.[60] Thus, the singular focus on threat actors, without regard to the locations of Australian citizens, was seen as establishing only a partial understanding of threat. As apparent from the US and Australian Committees findings, threat is more than simply an assessment of capability and intent.

Limitations of the conventional approach to assessing non-state threat were also evident in the investigation into the performance of the UK's intelligence and security agencies in relation to the London bombings. Indeed, of all the investigations, it is arguably the Intelligence and Security Committee which provides the greatest insight into the limits of the dominant episteme of threat. The ISC highlighted both the limits of collected information[61] and the lack of visibility of non-state threats as key issues limiting accurate assessments of non-state threats.[62] These conclusions were drawn from reflections on the nature of non-state threats and the difficulty of identifying and gaining understanding of these groups.

The core argument of this thesis is that Singer's model is too simplistic to capture the nature and complexity of non-state threats. As the purpose of the intent-capability model was the assessment of state-based threats, it does not factor in issues of either

[58] *Ibid.*, p.36.
[59] *Ibid.*, p.60.
[60] See *Ibid.*, Chapter 4.
[61] *Ibid.*, p.31.
[62] *Ibid.*, p.43.

identification or understanding of the threat actor. The well-defined and accepted nature of states differs with the often ill-defined and debatable nature of non-state actors. As evident in the three incidents looked at in the thesis, the identification and understanding of threat actors was critical in analysts' inability to accurately identify the threats which later manifest themselves. Singer's model does not capture the inherent complexity and uncertainty inherent in existing context of security within which individuals and small groups exercise mass-killing power indiscriminately. Evident in each of the Committees' conclusions is an acknowledgement that threat is more than just intent and capability.

Consequently, the nature and characteristics of non-state actors themselves actually limit the applicability of the conventional model. A fundamental requirement of accurately assessing non-state threats is identification; confirming that an actor exists. In addition, analysts must understand the group's nature and boundaries in order to assess the group's actual capabilities and intentions. Unlike assessments of state-based threats which rely on well-defined and well-known threat actors, intelligence agencies' in each of these incidents were faced with a lack of clear boundaries around organisations and ambiguous links between individuals and threatening groups. As the purpose of Singer's model was the assessment of state-based threats, the model does not factor in issues of either identification or understanding of the threat actor. Singer's model assumed that understanding of threat was simply a matter of looking at a state's military forces and political hierarchy to come to a conclusion about capability and intent. Thus, the conventional approach *commences* with intent and capability, with the threat actor is assumed to be already defined and understood. Such an assumption does not hold when assessing non-state threats. Indeed, the nature of these groups often defies understanding even if the group's existence is able to be identified, undermining, thereby, the

applicability of Singer's model.

8.3 A More Comprehensive Model of Threat

In Chapter 4, it was argued that there are alternatives to the conventional actor-based approach. Three alternatives were proposed: a vulnerability approach; an environment approach; and a situational approach. It was argued that elements of each of these approaches could be seen to be relevant to an expanded epistemology, ontology and methodology of threat. The argument is that these would provide a more comprehensive model of threat, better reflecting the complexity of a concept of threat. An examination of each of the three case studies highlighted the principal approach by intelligence agencies to consciously assessing non-state threats based on the conventional approach of *intentions* and *capabilities*. It was shown that elements of threat described in the vulnerability, environment and situational approaches were relevant to assessing non-state threats, with many factors *already* being used by intelligence analysts, albeit without these being consciously, deliberately or consistently applied. This highlights the potential to develop a more comprehensive model of threat which better reflects the difficulty in identifying the existence or development of non-state threat actors.

Conclusion

This study has provided a critique of the predominant concept of threat within intelligence analysis, that of Singer's model. Governments, intelligence agencies and researchers in the field continue to rely, almost exclusively, on Singer's approach for assessing both state-based and non-state threats. The re-thinking of Singer's model of threat in order to move beyond an uncritical acceptance of the conventional approach is, of itself, a novel and important contribution to the field of intelligence analysis.

The core argument of this thesis is that Singer's model is too simplistic to capture the nature and complexity of non-state threats. Singer's model requires ideal conditions for it to work. The bi-polar Cold War provided a framework which these conditions largely existed, with neatly defined state-based threats being the primary focus of intelligence analysis. This study amplifies the increasingly complex security environment within which non-state actors and states function, presenting and analysts with multiple threat assessment priorities, for which Singer's model has very little to say.

The difficulty of identifying unambiguous measures, proxy-measures and indicators for assessing non-state actors' capabilities and intentions to conduct mass-casualty attacks highlighted the analytical difficulty facing analysts. In contrast to the popular argument that threat assessment is simply a matter of shifting analytical focus between parameters when one parameter is deemed too difficult to measure or estimate, the study highlights that *both* parameters have significant and, potentially, unavoidable limitations and weaknesses in assessing non-state actors.

The lack of deliberate critiques of Singer's model was highlighted, with what might be termed as implicit critiques of the conventional approach being more accurately described as debates within the model; that is, arguments over which of the two parameters should be the primary focus of attention. Further, discussions over additional parameters (most notably *vulnerability* and *opportunity*) rest on the assumption that the parameters of *capability* and *intent* remain core to assessing threat. Two alternative approaches for assessing non-state threats were considered, namely vulnerability and environmental methodologies. These have not been considered as alternatives to the conventional approach in their own right but are evident within the literature, perhaps reflecting efforts to articulate the complexity of the concept of threat beyond the conventional approach.

Three incidents of mass-casualty attacks by non-state actors were critically examined to vivify the distinct and faceted aspects of the analytical problem of non-state threat. Limitations of Singer's approach to assessing non-state threat were particularly evident in the investigation into the performance of the UK's intelligence and security agencies in relation to the London bombings. Indeed, of all the investigations, it is arguably the Intelligence and Security Committee which provides the greatest insight into the limits of the dominant episteme of threat. The ISC highlighted both the limits of collected information and the lack of visibility of non-state threats as key issues limiting accurate assessments of non-state threats. Additionally, investigations into the London and Bali bombings indicated that analysts in both the UK and Australia actually did go beyond the conventional approach. Analysts drew upon factors external to specific groups in setting threat levels above what would have been warranted if relying solely upon known groups' capabilities and intentions. This, in itself, identifies that the intention-capability approach is too simplistic to capture the complexity of non-state threats. Instead, as presented in this

thesis, a more comprehensive model of threat appears worthy of further consideration. The approach would deliberately articulate and consider: the referent; the environment (factors external to both the referent and threat actor); situations and social environments within which threat actors might exist and emerge; as well as identified threat actors, albeit with a deliberate recognition of the limitations of the conventional approach.

Bibliography

Alberts, David, *Defensive Information Warfare*, National Defense University Press Book, Washington, D.C., August 1996.

Aldrich, Richard, *The Hidden Hand: Britain, America, and Cold War Secret Intelligence*, The Overlook Press, Woodstock, 2001.

Aldrich, Richard, 'Grow Your Own': Cold War Intelligence and History Supermarkets, *Intelligence and National Security*, No.17, Vol.1, March 2002, pp.133-152.

Alexseev, Mikhail, *Without Warning: Threat Assessment, Intelligence and Global Struggle*, Palgrave Macmillan, Houndmills, 1997.

Andrew, Christopher; Dilks, David, (Eds.), *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century*, University of Illinois Press, Urbana, 1984.

Andrew, Christopher, *Intelligence analysis needs to look backwards before looking forward*, June 2004, accessed on 23 December 2008 at: www.historyandpolicy.org/

Andrew, Christopher, Intelligence, International Relations and 'Under-theorisation', *Intelligence and National Security*, Vol.19, No.2, Summer 2004, pp.170-184.

Applegate, Melissa, *Preparing for Asymmetry: As seen through the lens of Joint Vision 2020*, Strategic Studies Institute, Carlisle, September 2001.

Armed Forces Communications and Electronics Association (AFCEA), Intelligence and the New National Security Environment, *Defense Intelligence Journal*, Vol.13, No.1&2, 2005, pp.17-38.

Armed Forces Communications and Electronics Association (AFCEA), Making Analysis Relevant: More than Connecting the Dots, *Defense Intelligence Journal*, Vol.14, No.1, 2005, pp.23-46.

Arquilla, John; Ronfelt, David (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, RAND, Santa Monica, 2001.

Ashworth, N., Threat Assessment, *Australian Defence Force Journal*, No.84, September/October 1990, pp.29-31.

Asi, Rohaiza, *Jemaah Islamiyah: An evolution in tactics or a weakening?*, IDSS Commentaries, 24 November 2005, accessed at: www.rsis.edu.sg/

Atran, Scott, The Genesis of Suicide Bombing, *Science*, Vol.299, 7 March 2003, pp.1534-1539.

Australian Defence Association, *Submission to the Parliamentary Joint Committee on ASIO, ASIS and DSD*, Inquiry into Certain Matters Relating to Iraq's Weapons of Mass

Destruction, 11 August 2003.

Aydinli, Ersel; and Rosenau, James (Eds.), *Globilization, Security and the Nation-State: Paradigms in Transition*, State University of New York Press, Albany, 2005.

Badey, Thomas, Nuclear Terrorism: Actor-based Threat Assessment, *Intelligence and National Security*, Vol.16, No.2, Summer 2001, pp.39-54.

Bailey, Jonathan, Strategy and Campaigning: End, Ways and Means, in (Ed.) Hopkins, Scott, *Asymmetry and Complexity: Selected Papers from the 2005 Rowell Seminar and the 2005 Chief of Army's Conference*, Land Warfare Studies Centre, Canberra, February 2007, pp.51-73.

Baker, John, Jemaah Islamiyah, in Brian Jackson et al (Eds.), *Aptitude for Destruction Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, RAND Corporation, Santa Monica, 2005.

Baldwin, David, Security Studies and the end of the Cold War, *World Politics*, No.48, October 2005, pp.117-141.

Ball, Desmond; Taylor, Brendan, Introduction in Williams, Clive; Taylor, Brendan (Eds.), *Countering Terror: New Directions Post '911'*, Strategic & Defence Studies Centre, Canberra, 2003.

Barno, David, Challenges in Fighting in a Global Insurgency, *Parameters*, Vol.36, Summer 2006, pp.15-29.

Barta, Paul, *Defence Update 2003 and the emerging terrorist threat*, Australian Command and Staff College, Canberra, Geddes Papers 2004.

Bartholomees, J. Boone (Ed.), *U.S. Army War College Guide to National Security Policy and Strategy*, Strategic Studies Institute, Second Ed., Carlisle, June 2006.

Baumard, Philippe, From Noticing to Making Sense: Using Intelligence to Develop Strategy, *International Journal of Intelligence and CounterIntelligence*, Vol.7, No.1, 1994, pp.29-73.

Beazley, Kim, Reorganisation of defence intelligence, Ministerial statement by the Minitster 1 March 1989, reported in *Australian Intelligence Magazine*, December 1989, pp.5-7.

Bell, J., Towards a Theory of Deception, *International Journal of Intelligence and CounterIntelligence*, Vol.16, No.2, Summer 2003, pp.244-279.

Bell, J, *Dragonwars: Armed Struggle and Conventions of Modern War*, Transaction Publishers, New Brunswick, 1999.

Bell, Carol, *Living with giants: Finding Australia's place in a more complex world*, Australian Strategic Policy Institute, Barton, 2005.

Bell, Coral, *The First War of the 21st Century: Asymmetric Hostilities and the Norms of Conflict*, SDSC Working Paper No.364, Canberra, December 2001.

Bell, Coral, *A World Out Of Balance: American Ascendancy and International Politics in the 21st Century*, Longueville Books, Double Day, 2003.

Bellamy, Christopher, 'Tools of Ill-Omen': The Shifted Conflict Paradigm and Reduced Role of Conventional Military Power, *Cambridge Review of International Affairs*, Volume 15, Number 1, 2002, pp.149-157.

Ben-Israel, Isaac, Philosophy and Methodology of Intelligence: The Logic of Estimative Process, *Intelligence and National Security*, Vol.4, No.4, October 1989, pp.660-718.

Benbow, Tim, *The Magic Bullet: Understanding the 'Revolution in Military Affairs'*, Brassey's, London, 2004.

Bennett, Bruce, Responding to Asymmetric Threats, in *New Challenges, New Tools for Defense Decisionmaking*, (Eds.) Johnson, Stuart; Libicki, Martin; and Treverton, Gregory, RAND Corporation, Santa Monica, 2003.

Berger, Brent; Giessmann, Hans, *Transnational Security Challenges in Southeast Asia: Departing from a Crossroads?*, Dialogue + Cooperation 3/2003 at: http://www.fes-globalization.org/

Bergert, Matt; Lindsay, Dan, Intelligence Preparations for Operations, *Small Wars and Infurgencies*, Vol.13, No.2, Summer 2002, pp.133-143.

Bergin, Anthony; Hall, Robert (Eds.), *Intelligence & Australian National Security*, Australian Defence Studies Centre, Canberra, 1994.

Berkowitz, Bruce, The New Protracted Conflict: Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, Pages 289-300.

Berkowitz, Bruce, Intelligence and the War on Terrorism, *Orbis*, Vol.46, No.2, Spring 2002, pp.289-300.

Betts, Richard, Analysis, War and Decision: Why Intelligence Failures are Inevitable, *World Politics*, Princeton University Press, Vol.31, No.1, October 1978, pp.61-89.

Betts, Richard, Intelligence Warning: Old Problems, New Agendas, *Parameters*, Spring 1998, pp.26-35.

Betts, Richard, Fixing Intelligence, *Foreign Affairs*, Vol.81, No.1, Jan/Feb 2002, pp.43-59.

Betts, Richard, The Soft Underbelly of American Primacy: Tactical Advantages of Terror, *Political Science Quarterly*, Vol.117, No.1, Spring 2002, pp.19-36.

Betts, Richard, Two Faces of Intelligence Failure: September 11 and Iraq's Missing WMD, *Political Science Quarterly*, Winter 2007/2008, Vol.24, No.4, pp.585-606.

Betz, David, Redesigning Land Forces for Wars Amongst the People, *Contemporary Security Policy*, Vol.28, No.2, August 2007, pp.221-243.

Bevan, James, Big Issue, Big Problem: MANPADS, *Small Arms Survey 2004: Rights at Risk*, accessed 2 July 2009 at:
http://www.smallarmssurvey.org/files/sas/publications/yearb2004.html

Black, Donald, The Geometry of Terrorism, *Sociological Theory*, Vol.22, No.1, March 2004, pp.14-25.

Blank, Stephen, *Rethinking Asymmetric Threats*, Strategic Studies Institute, Carlisle, September 2003.

Bobbitt, Philip, *The Shield of Achilles*, Penguin Group, London, 2003.

Bodnar, John, *Warning Analysis for the Information Age: Rethinking the Intelligence Process*, Joint Military Intelligence College, Washington, D.C., December 2003.

Bodnar, John, Making Sense of Massive Data by Hypothesis Testing, International Conference on Intelligence Analysis, McLean, Virginia, 2005.

Bolkcom, Christopher; Feickert, Andrew; and Elias, Bartholomew, *Homeland Security: Protecting Airliners from Terrorist Missiles*, Congressional Research Service, The Library of Congress, October 22, 2004.

Bolkcom, Christopher; Elias, Bartholomew; and Feickert, Andrew, *MANPADs Threat to Commercial Aviation*, accessed at: http://www.ifri.org/files/CFE/CFEbolkcom.pdf on 1 July 2009.

Boot, Max, *War Made New: Technology, Warfare, and the Course of History, 1500 to Today*¸ Gotham Books, New York, 2006.

Boot, Max, What are the Trends in International Security over the Next 20 Years?, *Australian Defence Force Journal*, No. 173, 2007, pp.13-24.

Bolt, Neville; Betz, David; and Azari, Jaz, *Propaganda of the Deed 2008: Understanding the Phenomenon*, Royal United Services Institute, Whitehall Report 3-08, 2008

Borgu, Aldo, *Australia's Defence after September 11*, Australian Strategic Policy Institute, Barton, 2001.

Borgu, Aldo, *Beyond Bali: ASPI's Strategic Assessment 2002*, Australian Strategic Policy Institute, Barton, 2002.

Borgu, Aldo, *Understanding Terrorism:20 basic facts*, Australian Strategic Policy Institute, Barton, September 2004.

Borum, Randy; Fein, Robert; Vossekuil, Bryan; Gelles, Michael; and Shumate, Scott, The Role of Operational Research in Counterterrorism, *International Journal of Intelligence and Counterlntelligence*, Vol.17, No.3, 2004, pp.420-434.

Boulding, Kenneth, Three Faces of Power, Sage Publications, Newbury Park, 1989.

Box, G.E.P., *Robustness in the Strategy of Scientific Model Building*, in Launer R.L., Wilkinson G.N. (Eds.) Robustness in Statistics: Proceedings of a Workshop. New York: Academic Press, 1979.

Boyd, Dallas; Dunn, Lewis; Arnold, Aaron; Ulrish, Michael; Scouras, James; and Fox, Jonathan, *Why Have We Not Been Attacked Again? Competing and Complementary Hypotheses for Homeland Security Attack Frequency*, Defense Threat Reduction Agency Advanced Systems and Concepts Office, Washington, D.C., June 2008.

Boyle, David, *The Tyranny of Numbers: Why Counting Can't Make Us Happy*, Harper Collins Publishers, London, 2001.

Breckinridge, Scott, The Shape of Post-Cold War Intelligence, *International Journal of Intelligence and CounterIntelligence*, Vol.8, No.1, Spring 1995, pp.1-10.

Brown, J., *Games 2000: Managing the Risks?*, Conference Paper, Canberra, 1995.

Burnett, Mark; Wooding, Pete; and Prekop, Paul, *Sense Making in the Australian Defence Organisation (ADO) Intelligence Community*, Defence Science and Technology Organisation, Canberra, 2005.

Burton, Fred; Stewart, Scott, *Disruption vs. Prosecution and the Manchester Plot*, accessed on 23 April 2009 at: www.stratfor.com/

Butler, Lord, *Review of Intelligence on Weapons of Mass Destruction: Report of a Committee of Privy Councillors*, House of Commons 898, London, The Stationery Office, 2004.

Busch, Kenneth; Weissman, Sidney, The Intelligence Community and the War on Terror: The Role of Behavioral Science, *Behavioral Sciences and the Law*, Vol.23, 2005, pp.559-571.

Buzan, Barry; Wæver, Ole; de Wilde, Jaap, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder, 1998.

Buzan, Barry; Segal, Gerald, *Anticipating the Future*, Simon and Schuster, London, 1998.

Campen, Alan, Low-tech humans subvert high-tech information assurance, *Signal*, Vol.56, No.5, pp.37-39.

Carroll, John, Twin Towers Revisited: A Cultural Interpretation of Modern Terrorism, *Australian Army Journal*, Vol.1, No.2, December 2003, pp.59-66.

Carpenter, William; and Wiencek, David (Eds.), *Asian Security Handbook: Terrorism and the New Security Environment*, 3rd Edition, M.E. Sharpe, New York, 2005.

Cavelty, Myriam; Mauer, Victor, Postmodern Intelligence: Strategic Warning in an Age of

Reflexive Intelligence, *Security Dialogue*, Vol.40, No.2, April 2009, pp.123-144.

Central Intelligence Agency, *Conference Report: Intelligence for a New Era in American Foreign Policy*, Center for the Study of Intelligence, January 2004.

Center for Security Studies, Emerging Threats in the 21st Century, *Strategic Foresight and Warning Seminar Series*, Final Report, Zurich, December 2007.

Center for Security Studies, Emerging Threats in the 21st Century, Seminar 2: Sense-Making and Warning – How to Understand and Anticipate Emerging Threats, *Strategic Foresight and Warning Seminar Series*, Final Report, Zurich, 19-21 January 2007.

Center for Security Studies, Emerging Threats in the 21st Century, Seminar 3: Warning for Readiness in the New Threat Environment, *Strategic Foresight and Warning Seminar Series*, Final Report, Zurich, 19-21 January 2007.

Chalk, Peter; Rosenau, William, *Confronting the "Enemy Within": Security Intelligence, the Police, and Counterterrorism in Four Democracies*, RAND, Santa Monica, 2004.

Charters, David; Farson, A.; Hastedt, Glenn (Eds.), *Intelligence Analysis and Assessment*, Frank Cass, London, 1996.

Chin, Warren, The United Kingdom and the War on Terror: The Breakdown of National and Military Strategy, *Contemporary Security Policy*, Vol.30, No.1, April 2009, pp.125-146.

Cilluffo, Frank; Marks, Ronald; and Salmoiraghi, George, The Use and Limits of U.S. Intelligence, in (Eds.) Loch Johnson and James Wirtz, *Strategic Intelligence: Windows Into a Secret World*, Roxby Publishing Company, Los Angeles, 2004.

Clark, Robert, *Intelligence Analysis: A Target-Centric Approach*, CQ Press, Washington, D.C., 2004.

Clarke, Peter, Lessons Learned from Terrorist Investigation in the United Kingdom, *RUSI Journal*, Vol.151, No.2, April 2006, pp.22-26.

Clements, Kevin, *Towards a Sociology of Security*, Conflict Research Consortium, Working Paper 90-4, July 1990, accessed on 6 October 2005 at: http://eprint.uq.edu.au/

Cobbold, Richard, Shocks and Surprises: Testing the Resilience, *RUSI Journal*, Col.150, No.4, August 2005, pp.4-6.

Cobbold, Richard, Knowing and Not Knowing, *RUSI Journal*, Vol.151, No.2, April 2006, pp.4-6.

Cobbold, Richard, Still Weaving the Tangled Web, *RUSI Journal*, Vol.151, No.4, August 2006, pp.4-7.

Cogan, Charles, Hunters not Gatherers: Intelligence in the Twenty-First Century, *Intelligence and National Security*, Vol.19, No.2, Summer 2004, pp.304-321.

Colwell, Rita, Science and Security in a Connected World, *Defense Intelligence Journal*, Vol.42, No.2, 2005, pp.37-44.

Cook, Malcolm, New uses of intelligence needed to counter terrorism, *RUSI/Jane's Homeland Security and Resilience Monitor*, 01 May 2004, accessed on 6 June 2005, at www.janes.com/

Coombe, Rodney, *Security in the post–Cold War Asia–Pacific*, Australian Defence College, Monograph Series, No. 2, 2003.

Cooper, Jeffrey, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., December 2005.

Corbin, Marcus, *Honing the Sword: Strategy and Forces after 9/11*, Center for Defense Information, Washington D.C., February 2003.

Cordesman, Anthony, *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the U.S. Homeland*, Centre for Strategic and International Studies, Washington, D.C., 2002.

Cordesman, Anthony, *The War After the War: Strategic Lessons of Iraq and Afghanistan*, Centre for Strategic and International Studies Press, Washinton, D.C., 2006.

Corera, Gordon, Radical reform required in US intelligence community, *Jane's Intelligence Review*, April 2004, pp.42-47.

Cradock, Percy, *Know Your Enemy: How the Joint Intelligence Committee Saw the World*, John Murray, London, 2002.

Cragan, Kim; Daly, Sarah, The Dynamic Terrorist Threat: An Assessment of Group Motivations and Capabilities in a Changing World, RAND, Santa Monica, 2004.

Craig, Alexander, *The Joint Intelligence Committee and British Intelligence Assessment, 1945-1956*, unpublished PhD thesis, July 1999.

Criminal Intelligence Service Canada, *Strategic Early Warning for Criminal Intelligence: Theoretical Framework & Sentinel Methodology*, Ottawa, 2007.

Crumpton, Henry Intelligence and Homeland Security, in Sims, Jennifer; and Gerber, Burton (Eds.), *Transforming U.S. Intelligence*, Georgetown University Press, Washington, D.C., 2005.

Daase, Christopher; and Kessler, Oliver, Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger, *Security Dialogue*, Vol. 38, No. 4, 2007, pp. 411-434.

D'Agostino, Mark; Martin, Greg, The bioscience revolution and the biological weapons threat: levers and interventions, *Globalization and Health*, Vol.5, No.3, accessed on 20

April 2009 at: www.globalizationandhealth.com/

Dahl, Erik, Warning of Terror: Explaining the Failure of Intelligence Against Terrorism, *The Journal of Strategic Studies*, Vol.28, No. 1, 31 – 55, February 2005.

Dannatt, Richard; A Perspective on the Nature of Future Conflict, 15 May 2009, accessed at: http://www.chathamhouse.org.uk/files/14009_150509dannatt.pdf

Davies, Philip, Intelligence Culture and Intelligence Failure in Britain and the United States, *Cambridge Review of International Affairs*, Vol.17, No.3, October 2004, pp.495-520.

Davis, Jack, *Improving CIA Analytic Performance: Strategic Warning*, Sherman Kent Center for Intelligence Analysis, Occasional Papers: Vol.1, No.1, September 2002.

Davis, Jack, *Strategic Warning: If Surprise is Inevitable, What Role for Analysis?*, Sherman Kent Center for Intelligence Analysis, Occasional Papers: Vol.2, No.1, January 2003.

Davis, Paul; Jenkins, Brian, *Deterrence and Influence in Counterterrorism: A Component in the War on Al Qa'ida*, RAND, Santa Monica, 2002.

Davis, Paul; and Jenkins, Brian, *Deterrence and Influence in Counterterrorism: A Component in the War on Al Qa'ida*, RAND Corporation, Santa Monica, 2002.

Dearlove, Richard; Quiggin, Tom, *Contemporary Terrorism and Intelligence*, IDSS Commentaries, 7 August 2006, accessed at: www.rsis.edu.sg/

Delpech, Therese, The Imbalance of Terror, *The Washington Quarterly*, Vol.25, No.1, Winter 2002, pp.31-40.

Derksen, Kevin, Commentary: The Logistics of Actionable Intelligence Leading to 9/11, *Studies in Conflict & Terrorism*, Vol.28, 2005, pp.253-268.

Dick, Charles, *Conflict in a Changing World*, Conflict Studies Research Centre, August 2000.

Dupont, Alan, *Australia's Threat Perceptions: A Search for Security*, Strategic and Defence Studies Centre, Canberra, 1991.

Dupont, Alan, Transformation or stagnation? Rethinking Australia's defence, *Australian Journal of International Affairs*, Vol. 57, No. 1, 2003, pp. 55–76, p.55.

Dupont, Alan, Grand Strategy, National Security and the Australian Defence Force, *Lowy Institute Perspectives*, May 2005 accessed at: www.lowyinstitute.org/

Durodie, Bill, Perception and Threat: Why Vulnerability-led Responses will Fail, *RUSI/Jane's Homeland Security and Resilience Monitor*, 1 November 2002, accessed on 11 February 2005 at: www.janes.com/

Duyvesteyn, Isabelle, How New Is the New Terrorism?, *Studies in Conflict & Terrorism*, Vol.27, No.5, 2004, pp.439-454.

Dylan, Huw, Britain and the Missile Gap: British Estimates on the Soviet Balistic Missile Threat, 1957-61, *Intelligence and National Security*, Vol.23, No.6, 2008, pp.777-806.

Echevarria, Antulio, *The Army and Homeland Security: A Strategic Perspective*, Strategic Studies Institute, Carlisle Barracks, March 2001.

Ellis, Brent, Countering Complexity: An Analytical Framework to Guide Counter-Terrorism Policy-Making, in in Russell Howard and Reid Sawyer (Eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004.

Enemark, Christian, *The Biological Terrorist: Willing and Able to Cause Mass Casualties?*, Paper presented at the Oceanic Conference on International Studies, 14-16 July, Australian National University.

Evangelista, Matthew, The "Soviet Threat": Intentions, Capabilities, and Context, *Diplomatic History*, Vol.22, No.3, Summer 1998, pp.439-449.

Evans, Jonathan, *MI5 Director General's Speech on Intelligence, Counter-Terrorism and Trust*, 5 November 2007, accessed at: www.cfr.org/publication/14789/mi5_director_generals_speech_on_intelligence_counterterrorism_and_trust_html on 9 May 2009.

Evans, Michael; Ryan, Alan; Parkin, Russell (Eds.), *Future Armies, Future Challenges: Land warfare in the information age*, Allen & Unwin, 2004.

Fealy, Greg; Borgu, Aldo, *Local Jihad: Radical Islam and terrorism in Indonesia*, Australian Strategic Policy Institute**,** Barton, September 2005.

Ferris, John, *Intelligence and Strategy*, Routledge, London, 2005.

Financial Action Task Force, *Terrorist Financing*, 29 February 2009, available at: http://www.fatf-gafi.org/dataoecd/28/43/40285899.pdf accessed on 3 July 2009.

Fishbein, Warren; and Treverton, Gregory, *Making Sense of Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.1, October 2004.

Fishbein, Warren; and Treverton, Gregory, *Rethinking "Alternative Analysis" to Address Transnational Threats*, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, Vol.3, No.2, October 2004, accessed on 12 June 2009, at: www.cia.gov/

FitzGibbon, Constantine, *Secret Intelligence in the Twentieth Century*, Hart-Davis MacGibbon, London, 1976.

Flaherty, Cristopher, Decisive Strike, Criticality and Homeland Security, *Australian Defence Force Journal*, No.164, 2004, pp.43-50.

Floridi, Luciano, Is Semantic Information Meaningful Data?, *Philosophy and Phenomenological Research*, Vol.70, No.2, March 2005, pp.351-370.

Flynn, Michael; Pottinger, Matthew; and Batchelor, Paul, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Centre for a New American Security, Washington, D.C., January 2010.

Flynt, Bill, Threat Kingdom, *Military Review*, July-August, 2000, pp.12-21.

Freedman, Lawrence, *The Evolution of Nuclear Strategy*, St Martin's Press, New York, 1983, referred to in Evans, Michael, Conventional Deterrence in the Australian Strategic Context, Land Warfare Studies Centre, Canberra, Working Paper No. 103, May 1999.

Freeman, Chas, *Arts of Power: Statecraft and Diplomacy*, United States Institute of Peace Press, Washington, D.C., 1997.

Fricker, Philip, Information and terrorism: from highway to boundary, *RUSI/ Jane's Homeland Security and Resilience Monitor*, 01 September 2005, accessed on 21 January 2006 at: www.janes.com/

Friedman, Thomas, *The Lexus and the Olive Tree*, Farrar, Strauss and Giroux, New York, 2000.

Friedman, George, *America's Secret War*, Doubleday, New York, 2004.

Frühling, Stephan, *A History of Australian Strategic Policy Since 1945*, Defence Publishing Service, Canberra, 2009.

Fukuyama, Francis, The End of History?, *The National Interest*, No.16, Summer 1989, pp.3-18.

Fuller, Fred, New Order Threat Analysis, *Marine Corps Gazette*, Vol. 81, No.4, April 1997.

Gale, Stephen, *Standards of Intelligence Reasoning*, Foreign Policy Research Institute, E-Notes, 14 November 2003, accessed on 22 December 2005 at: http://www.fpri.org/

Gale, Stephen, *Terrorism 2005: Overcoming the Failure of Imagination*, Foreign Policy Research Institute, E-Notes, 16 August 2005, accessed on 22 December 2005 at: http://www.fpri.org/

Ganor, Boaz, The Changing Threat of International Terrorism, *The Sydney Papers*, Winter 2002, pp.43-51.

Garthoff, Raymond, *On Estimating and Imputing Intentions*, International Security, Vol.2, No.3, Winter 1978, pp.22-32.

Gasper, Peter, *Cyber Threat to Critical Infrastructure 2010-2015: Increased Control System Exposure*, Idaho National Laboratory, available at:

http://usacac.army.mil/CAC2/CEW/repository/presentations/15_Idaho_Natl_Lab_IACS-CI_Threat_2010-2015.pdf accessed 4 Feb 2010.

George, Roger, Fixing the Problem of Analytical Mind-Sets: Alternative Analysis, *International Journal of Intelligence and CounterIntelligence*, Vol.17, 2004, pp.385-404.

George, Roger; Kline, Robert, *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, Rowan & Littlefield Publishers, Lanham, 2006.

Gibson, Stevyn, Open Source Intelligence: An Intelligence Lifeline, *RUSI Journal*, Vol.149, No.1, February 2004, pp.16-22.

Gill, Peter, Securing the Globe: Intelligence and the Post-9/11 Shift from 'Liddism' to 'Drainism', *Intelligence and National Security*, Vol.19, No.3, Autumn 2004, pp.467-489.

Gill, Peter; Phythian, Mark, *Intelligence in an Insecure World*, Polity Press, Cambridge, 2006.

Giustozzi, Antonio, Conflicting intelligence clouds assessments of Iraqi insurgency, *RUSI/Jane's Homeland Security and Resilience* Monitor, 01 April 2005, accessed on 21 January 2006 at: www.janes.com/

Gladwell, Malcolm, Connecting the Dots, accessed on 11 January 2006 at: www.newyorker.com/

Goodman, Melvin, 9/11: The Failure of Strategic Intelligence, *Intelligence and National Security*, Vol.18, No.4, Winter 2003, pp.59-71.

Goodman, Michael, *Studying and Teaching About Intelligence: The Approach in the United Kingdom*, accessed on 16 February 2009 at: www.cia.gov/

Gorka, Sebestyen, Closing the gaps in capability and threat perception, *Jane's Intelligence Review*, 01 July 2002, accessed on 11 February 2005 at: www.janes.com/

Grabo, Cynthia *Anticipating Surprise: Analysis for Strategic Warning*, University Press of America, Maryland, 2004.

Grau, Lester, Something Old, Something New: Guerrillas, Terrorists, and Intelligence Analysis, *Military Review*, Vol.84, No.4, July-August 2004, pp.42-49.

Gray, Colin, Thinking asymmetrically in times of terror, *Parameters*, Vol.32, No.1, Spring 2002, pp.5-15.

Gray, Colin, How Has War Changed Since the End of the Cold War, *Parameters*, Spring 2005, pp. 14-26.

Greavette, Gordon, *Terrorism in the Twentieth Century: The Evolution From a Subnational to a Transnational Entity*, accessed on 17 May 2007 at: http://www.cda-cdai.ca/symposia/2003/greavette.htm

Gressang, Daniel, Audience and Message: Assessing Terrorist WMD Potential, in (Ed.) O'Day, Alan, *Weapons of Mass Destruction and Terrorism*, Ashgate, Aldershot, 2004.

Gressang, Daniel, The Shortest Distance Between Two Points Lies in Rethinking the Question: Intelligence and the Information Age Technology Challenge in in Loch Johnson (Ed.), *Strategic Intelligence 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, Praeger Security International, Westport, 2007.

Grono, Nicholas, Australia's Response to Terrorism, *Studies in Intelligence*, Vol.48, No.1, pp.27-38.

Gunaratna, Rohan, The al-Qaeda Threat and the International Response in Jones, David (Ed.), *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004.

Gudgin, Peter, *Military Intelligence: A History*, Sutton Publishing, Thrupp, 1999.

Gustafson, Kristian, Strategic Horizons: Futures Forecasting and the British Intelligence Community, *Intelligence and National Security*, Vol.25: No.5, 20101, pp.589 – 610.

Gurr, Ted, *Methodologies and Data for the Analysis of Oppositional Terrorism*, Paper prepared for the Symposium on International Terrorism, Defense Intelligence College, Washington D.C., December 1985.

Haines, Gerald; Leggett, Robert (Eds.), *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*, Central Intelligence Agency, Center for the Study of Intelligence, Washington, D.C., 2003.

Handel, Michael, *War, Strategy, and Intelligence*, Frank Cass and Company Limited, Totowa, 1989.

Hansen, James, U.S. Intelligence Confronts the Future, *International Journal of Intelligence and CounterIntelligence*, Vol.17, 2004, pp.673-709.

Harrington, Simon, The Next Big Challenges, in *Scoping Studies: New thinking on security*, Australian Strategic Policy Institute, Barton, October 2004.

Hart, Douglas; Simon, Steven, Thinking Straight and Talking Straight: Problems of Intelligence Analysis, *Survival*, Vol.48, No.1, Spring 2006, pp.35-60.

Hastedt, Glenn, Estimating Intentions in an Age of Terrorism: Garthoff Revisited, *Defense Intelligence Journal*, Vol.14, No.1, 2005, pp.47-62.

Hayes, Joseph, Afterword, in Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, The Center for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2005.

Hendrickson, Noel, Critical Thinking in Intelligence Analysis, *International Journal of Intelligence and Counterintelligence*, Vol21, No.4, 2008, pp.679-693.

Heng, Yee-Kuang, The Return of Net Assessment, *Survival*, Vol.49, No.4, Winter 2007-08, pp.135-152.

Hennessey, Peter, *The Secret State: Whitehall and the Cold* War, Penguin Books, London, 2003.

Herbert, Matthew, The Intelligence Analyst as Epistemologist, *International Journal Of Intelligence and Counterintelligence*, Taylor & Francis Group, Vol.19, 2006, pp.666-684.

Herman, Michael, *Intelligence power in peace and war*, Cambridge University Press, Cambridge, 1996.

Heuer, Richards, *The Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 1999.

Heuer, Richards, Limits of Intelligence Analysis, *Orbis*, Vol.49, No.1, Winter 2005, pp. 75-94.

Highland, Grant, New Century, Old Problems: The Global Insurgency within Islam and the Nature of the War on Terror, in *Essays 2003: Chairman of the Joint Chiefs of Staff Strategy Essay Competition*, National Defense University Press, Washington, D.C., 2003.

Hirschfeld, Thomas, *Intelligence and Arms Control: A Marriage of Convenience*, Lyndon B. Johnson School of Public Affairs, 1987.

Hirschfeld, Thomas, Exaggerating Threats Shortchanges the Future, *U.S. Naval Institute Proceedings*, Vol.128, No.9, September 2002, pp.66-69.

Hitz, Frederick and Weiss, Brian, Helping the CIA and FBI Connect the Dots in the War on Terror, *International Journal of Intelligence and Counter Intelligence*, Vol.17, 2004, pp.1-41.

Hoffman, Bruce, *"Holy Terror": The Implications of Terror Motivated by a Religious Imperative*, RAND, Santa Monica, 1993.

Hoffman, Bruce, *Inside Terrorism*, Columbia University Press, New York, 1998.

Hoffman, Bruce, *Combating Terrorism: In Search of a National Strategy*, presented to the Subcommittee on National Security, Veterans Affairs, and International Relations, House Committee on Government Reform, March 27, 2001, RAND, Santa Monica, March 2001.

Hoffman, Bruce, *Lessons of 9/11*, submitted on 8 October 2002 for the Committee Record, U.S. Congress Joint Inquiry into Intelligence Activities Before and After the Attacks on September 11, 2001, RAND, Santa Monica, October 2002.

Hoffman, Bruce, Rethinking Terrorism and Counterterrorism Since 9/11, *Studies in Conflict and Terrorism*. Vol.25, 2002, pp.303-316.

Hoffman, Bruce, Al Qaeda, Trends in Terrorism, and the Future Potentialities: An

Assessment, *Studies in Conflict and Terrorism*, Vol.26, 2003, pp.429-442.

Hoffman, Bruce, *Combating Al Qaeda and the Militant Islamic Threat*, Testimony presented to the House Armed Services Committee, Subcommittee on Terrorism, Unconventional Threats and Capabilities on February 16, 2006, RAND, Santa Monica, 2006.

Hoffman, Bruce, The Myth of Grassroots Terrorism: Why Osama bin Laden Still Matters, *Foreign Affairs*, Vol.87, 2008, pp.133-138.

Hoffman, Bruce, Assessing the State of Al Qaeda and Current and Future Terrorist Threats, in Karawan, Ibrahim; McCormack, Wayne; and Reynolds, Stephen (Eds.), *Values and Violence: Intangible Aspects of Terrorism*, Studies in Global Justice, Vol.4, Springer, 2008.

Hoffman, Bruce, The Evolving Nature of Terrorism – Nine Years after the 9/11 Attacks, *The Social Contract*, Vol.21, No.1, Fall 2010, pp.33-40.

Hollister, John, The Challenges of Intelligence Analysis, in Lock Johnson (Ed.), *Strategic Intelligence 1: Understanding the Hidden Side of Government*, Praeger Security International, Westport, 2007.

Hollywood, John; Snyder, Diane; McKay, Kenneth; and Boon, John, *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior*, RAND Corporation, Santa Monica, 2004.

Horowitz, Barry; Haimes, Yacov, Risk-Based Methodology for Scenario Tracking, Intelligence Gathering and Analysis for Countering Terrorism, *Systems Engineering*, Vol.6, No.3, 2003, pp.152-169.

Hough, Peter, *Understanding Global Security*, Routledge, London,

Houston, Angus, The ADF of the Future, *Australian Defence Force Journal*, No. 173, 2007, pp.57-67.

Howard, Michael, "9/11" and after: A British view, *Naval War College Review*; Autumn 2002; Vol.55, No.4, pp.10-20.

Howard, Russell and Sawyer, Reid, *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004.

Hughes, Christopher, Japan's Aum Shinrikyo, in Ried, Anna (Ed.), *Taming Terrorism: It's Been Done Before*, Policy Exchange, London, 2004.

Hulnick, Arthur, What's Wrong with the Intelligence Cycle, *Intelligence and National Security*, Vol.21, No.6, December 2006, pp.959-979.

Hulnick, Arthur, Indications and Warning for Homeland Security: Seeking a New Paradigm, *International Journal of Intelligence and CounterIntelligence*, Vol.18, 2005, pp.593–608.

Hunter, Thomas, The proliferation of MANPADS, *Jane's Intelligence Review*, 28 November 2002.

Huntington, Samuel, *The Soldier and the State: The Theory and Politics of Civil-Military Relations*, Vintage Books, New York, 1957.
Immerman, Richard, A Brief History of the CIA, Athan Theoharis, Richard Immerman, Loch Johnson, Kathryn Olmsted, and John Prados (Eds.), *The Central Intelligence Agency: Security Under Scrutiny*, Greenwood Press, Westport, 2006.

International Atomic Energy Agency report accessed on 3 July 2009 at: http://www-ns.iaea.org/security/itdb.htm.

Jackson, Brian; Baker, John; Chalk, Peter; Cragin, Kim; Parachini, John; Trujillo, Horacio, *Aptitude for Destruction Volume 1: Organizational Learning in Terrorist Groups and Its Implications for Combating Terrorism*, RAND Corporation, Santa Monica, 2005.

Jackson, Brian; Baker, John; Chalk, Peter; Cragin, Kim; Parachini, John; Trujillo, Horacio, (Eds.), *Aptitude for Destruction Volume 2: Case Studies of Organizational Learning in Five Terrorist Groups*, RAND Corporation, Santa Monica, 2005.

Jackson, Brian, Groups, Networks, or Movements: A Command-and-Control-Driven Approach to Classifying Terrorist Organizations and Its Application to Al Qaeda, *Studies in Conflict & Terrorism*, Vol.29, 2006, pp.241–262.

Jane's World Armies, available by subscription accessed on 30 June 2010 at: http://jwar.janes.com/

Jane's Information Group, More attacks - or paranoia?, *Jane's Intelligence Digest*, October 2001, accessed on 10 January 2005 at: www.janes.com/

Janes' Information Group, The threat of domestic terrorism, *Jane's Terrorism & Security Monitor*, 18 May 2005, accessed on 23 May 2005 at: www.janes.com/

Jane's Information Group, The 7 July bombings: the unanswered questions, *Jane's Terrorism and Security Monitor*, 14 June 2006, accessed on 29 June 2006 at: www.janes.com/

Janes' Information Group, Al-Qaeda online: understanding jihadist internet infrastructure, *Janes Intelligence Review*, 01 January 2006, accessed on 31 March 2006 at: www.janes.com/

Jeffreys-Jones, Rhodri; Andrew, Christopher, (Eds.), *Eternal Vigilance? 50 Years of the CIA*, Frank Cass, London, 1997.

Jenkins, Brian, Redefining the Enemy: The World has Changed, But Our Mindset Has Not, *RAND Review*, Vol.28, Spring 2004, accessed on 17 June 2008 at: www.rand.org/

Jenkins, Brian; Treverton, Gregory, *Misjudging The Jihad: Briefing Osama on All the War's Wins and Losses*, RAND, Santa Monica, 2005.

Jenkins, Brian, *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica, 2006.

Jennings, Peter, *Beyond Baghdad: ASPI's Strategic Assessment 2004*, Australian Strategic Policy Institute, Barton, 2004.

Jennings, Peter, Unfinished Business: Reforming our Intelligence Agencies, *Policy*, Vol.20, No.4, Summer 2004-05, pp.3-8.

Jervis, Robert, What's Wrong with the Intelligence Process?, *International Journal of Intelligence and CounterIntellignce*, Vol.1, No.2, Spring 1986, pp.28-41.

Johnson, Rob, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2005.

Johnson, Loch, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*, New York University Press, New York, 2000.

Johnson, Loch, Preface to a Theory of Strategic Intelligence, *International Journal of Intelligence and CounterIntelligence*, Vol.16, 2003, pp.638-663.

Johnson, Loch; Wirtz, James (Eds.), *Strategic Intelligence: Windows Into a Secret World*, Roxby Publishing Company, Los Angeles, 2004.

Johnson, Loch, An Introduction to the Intelligence Studies Literature, in *Strategic Intelligence 1: Understanding the Hidden Side of Government*, ed. Loch Johnson (Ed.), Praeger Security International, Westport, 2007.

Johnson, Loch (Ed.), *Strategic Intelligence 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, Praeger Security International, Westport, 2007.

Johnson, Loch (Ed.), *Strategic Intelligence 4: Counterintelligence and Counterterrorism: Defencing the nation against hostile forces*, Praeger Security International, Westport, 2007.

Johnston, Rob, Integrating Methodologists into Teams of Substantive Experts: Reducing Analytic Error, *Studies in Intelligence*, Vol. 47, No 1, 2003, pp.57-65.

Jonas, Jeff; Harper, Jim, Effective Counterterrorism and the Limited Role of Predictive Data Mining, *Policy Analysis*, CATO Institute, No.584, 11 December 2006.

Jones, Bruce, Technology moves modern battlespace into cyberspace, *RUSI/Jane's Homeland Security and Resilience* Monitor, 01 November 2005, accessed on 21 January 2006 at: www.janes.com/

Jones, Christopher, The CIA Under Clinton: Continuity and Change, *International Journal of Intelilgnece and CounterIntelligence*, Vol.14, No.4, 2001, pp.503-528.

Jones, David; Smith, Michael; and Weeding, Mark, Looking for the Pattern: *Al Qaeda* in Southeast Asia – The Genealogy of a Terror Network, *Studies in Conflict & Terrorism*, Vol.26, 2003, pp.443-457.

Jones, R.V., The Theory of Practical Joking – An Elaboration, *The Bulletin of the Institute of Mathematics and It's Applications*, Vol.11, No.1/2, Jan/Feb 1975, pp.10-17.

Jones, R.V., *Reflections on Intelligence*, William Heinemann, London, 1990.

Jones, Sidney The changing nature of Jemaah Islamiyah, *Australian Journal of International Affairs*, Vol. 59, No. 2, June 2005, pp. 169–178.

Jones, Sidney, *The Changing Face of Terrorism in Indonesia: Weaker, More Diffuse, and Still a Threat*, Speech to the Australian Strategic Policy Institute, 15 September 2005 at: http://www.crisisgroup.org/en/publication-type/speeches/2005/the-changing-face-of-terrorism-in-indonesia-weaker-more-diffuse-and-still-a-threat.aspx.

Jost, Patrick; and Sandhu, Harjit, *The hawala alternative remittance system and its role in money laundering*, January 2000, accessed on 2 March 2011 at: www.interpol.int/

Juarrero, Alicia, *Dynamics in Action: Intentional Behavior as a Complex System*, MIT Press, Cambridge, 2002.

Kan, Paul, The Blurring Distinction Between War and Crime in the 21st Century: Breaking the Target Selection Paradigm in a Globalizing World, *Defense Intelligence Journal*, Vol.13, No.1&2, 2005, pp.39-45.

Kahan, Ephraim, Early Warning versus Concept: The Case of the Yom Kippur War 1973, *Intelligence and National Security*, Vol.17, No.2, Summer 2002, pp.81-104.

Kerbel, Josh, Thinking Straight: Cognitive Bias in the US Debate about China, *Studies in Intelligence*, Vol. 48, No. 3, 2004, pp.27-35.

Khalsa, Sundri, *Forecasting Terrorism: Indicators and Proven Analytic Techniques*, Scarecrow Press Inc., Maryland, 2004.

Khan, David, *Hitler's Spies: German Military Intelligence in World War II*, Macmillan, 1978.

Khan, David, The Intelligence Failure of Pearl Harbor, *Foreign Affairs*, Winter 1991/1992, Vol.70, Issue 5, pp.138-152.

Khan, David, An Historical Theory of Intelligence, *Intelligence and National Security*, Vol.16, No.3, Autumn 2001, pp.79-92.

Kahn, David, The Rise of Intelligence, *Foreign Affairs*, Sep/Oct 2006, Vol. 85, No.5, pp.125-134.

Kaplan, Robert, *The Coming Anarchy*, The Atlantic Monthly, February 1994.

Karber, Phillip; Combs, Jerald, The United States, NATO, and the Soviet Threat to Western Europe: Military Estimates and Policy Options, 1945-1963, *Diplomatic History*, Vol.22, No.3, Summer 1998, pp.399-429.

Kent, Sherman, *Strategic Intelligence for American World Policy*, revised edition, Princeton University Press, 1966.

Kent, Sherman, *The Need for an Intelligence Literature*, CIA Center for the Study of Intelligence, accessed 11 February 2010 at: www.cia.gov/

Kent, Sherman, *A Crucial Estimate Relived*, Center for the Study of Intelligence, accessed on 10 March 2011 at: www.cia.gov/

Kent, Sherman, *Words of Estimative Probability*, Center for the Study of Intelligence, accessed on 5 January 2006 at: www.odni.gov/

Kilcullen, David, *Countering Global Insurgency*, 30 November 2004, accessed on 17 June 2006 at: http://smallwarsjournal.com/documents/kilcullen.pdf

Kilcullen, David, *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Scribe, Melbourne, 2009.

Kiras, James, Terrorism and Irregular Warfare, in Baylis, John; Wirtz, James; and Gray, Colin (Eds.), *Strategy in the Contemporary World: An Introduction to Strategic Studies*, Oxford University Press, Oxford, 2002.

Klein, Gary; Moon, Brian; and Hoffman, Robert, Making Sense of Sensemaking 1: Alternative Perspectives, *IEEE Intelligent Systems*, Vol. 21, No. 4, July/August 2006, pp.70-73.

Krahmann, Elke, From State to Non-State Actors: The Emergence of Security Governance, in ed. Elke Krahmann, *New Threats and New Actors in International Security*, Palgrave MacMillan, New York, 2005.

Krulak, Charles, The Strategic Corporal: Leadership in the Three Block War, *Marines Magazine*, January 1999.

Kurtz, Cynthia; and Snowden, David, The new dynamics of strategy: Sense-making in a complex and complicated world, *IBM Systems Journal*, Vol.42, No.3, 2003, pp.462-483.

Lahneman, William, Knowledge-Sharing in the Intelligence Community After 9/11, *International Journal of Intelligence and CounterIntelligence*, Vol.17, No.4, 2004, pp.614–633.

Lanning, Michael, *Senseless Secrets: The Failures of U.S. Military Intelligence, From George Washington to the Present*, Carol Publishing Group, New York, 1996.

Laqueur,Walter, *The Uses and Limits of Intelligence*, Transaction Publishers, New Brunswick, 1993.

Laqueur, Walter, *No End to War: Terrorism in the Twenty-First Century*, The Continuum International Publishing Group Inc, 2003.

Layton, Peter, Redefining Warfare, *Royal United Services Institute Journal*, Feb 2007, Vol 152, No.1, pp.34-41.

Leary, William (Ed.), *The Central Intelligence Agency: History and Documents*, University of Alabama Press, 1984.

Lefebvre, Stephane, A Look at Intelligence Analysis, *International Journal of Intelligence and CounterIntelligence*, Vol.17, No.2, 2004, pp.231-264.

Leffler, Melvyn, The American Conception of National Security and the Beginnings of the Cold War, American Historical Review, Vol.89, No.2, April 1984, pp.346-381.

Leitenberg, Milton, *Deaths in Wars and Conflicts in the 20th Century*, 3rd Edition, Cornell University Peace Studies Program, Occasional Paper No.29, 2006 at: http://www.clingendael.nl/publications/2006/20060800_cdsp_occ_leitenberg.pdf.

Lesser, Ian; Hoffman, Bruce; Arquilla, John; Ronfeldt, David; Zanini, Michele; Jenkins, Brian, *Countering the New Terrorism*, RAND, Santa Monica, 1999.

Leschen, Peter, *The nature of future conflict and its impact on Australia's defence policy and force structure*, Australian Defence College, Canberra, Monograph Series No.6, 2004.

Lia, Brynjar, *Globalisation and the Future of Terrorism: Patterns and Predictions*, Routledge, London, 2005.

Liang, Qiao; Xiangsui, Wang, *Unrestricted Warfare*, PLA Literature and Arts Publishing House, Beijing, February 1999.

Little, Eric; and Rogova, Galina, An Ontological Analysis of Threat and Vulnerability, in *9th International Conference on Information Fusion*, 10-13 July 2006.

Lonsdale, David, *The Nature of War In The Information Age: Clausewitzian Future*, Frank Cass, London, 2004.

Lowenthal, Mark *Intelligence: From Secrets to Policy*, 3rd Edition, CQ Press, Washington, D.C., 2006.

Ludwick, Keith, *Closing the Gap: Measuring the Social Identity of Terrorists*, Naval Postgraduate School, Monterey, California, September 2008.

Luikart, Kenneth; and Ang, Georgia, Transforming homeland security: Intelligence indications and warning, *Air and Space Power Journal*, Vol.17, No.2, Summer 2003, pp.69-78.

Lyon, Rod, Six Challenges, in *Scoping Studies: New thinking on security*, Australian Strategic Policy Institute, Barton, 2004.

Lyon, Rod, *Alliance Unleashed: Australia and the US in a new strategic age*, Australian Strategic Policy Institute, Barton, 2005.

MacEachin, Douglas, Analysis and Estimates: Professional Practices in Intelligence Production, in eds. Sims, Jennifer; and Gerber, Burton, *Transforming U.S. Intelligence*, Georgetown University Press, Washington, D.C., 2005.

Macquarie Dictionary, 5th Edition, Macquarie Dictionary Publishers, Sydney, 2009.

Mandel, Robert, On Estimating Post-Cold War Enemy Intentions, *Intelligence and National Security*, Vol.24, No.2, 2009, pp.194-215.

Manningham-Buller, Eliza, *Speech By The Director General of the Security Service, Dame Eliza Manningham-Buller, At The Ridderzaal, Binnenhof, The Hague, Netherlands*, 1 September 2005, accessed on 11 February 2010 at: https://www.mi5.gov.uk/output/director-generals-speech-to-the-aivd-2005.html.

Manningham-Buller, Eliza, *Terrorist Threat to the UK: MI5 Chief's full speech*, 9 November 2006, Times Online, published 10 November 2006.

Marrin, Stephen, Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities, *Intelligence and National Security*, Vol.22, No.6, December 2007, pp.821-846.

Marrin, Stephen, CIA's Kent School: Improving Training for New Analysts, *International Journal of Intelligence and CounterIntelligence*, Vol.16, No.4, 2003, pp.609-637.

May, Ernest, Intelligence: Backing into the Future, *Foreign Affairs*, Vol.71, No.3, Summer 1992, pp.63-72.

McCaffrey, Barry; Basso, John, Narcotics, Terrorism, and International Crime: The Convergence Phenomenon, in Russell Howard and Reid Sawyer (Eds.), *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004.

McConnell, Mike, Overhauling Intelligence, *Foreign Affairs*, Vol. 86, No.4, July/August 2007, pp.49-58.

McIntrye, Dave, Homeland Security: What Is to Be Done, *Military Technology*, Vol.15, No.12, 2001, pp.12-21.

McKenzie, Kenneth, *The Revenge of the Melians: Asymmetric Threats and the Next QDR*, Institute for National Strategic Studies, McNair Paper No.62, Washington, D.C., 2000.

McNeill, Joseph, *Unshackling the Sphinx: Intelligence in the Post-9/11 World*, US Army War College, Carlisle, 2005.

Medby, Jamison; and Glenn, Russell, *Street Smart: Intelligence Preparation of the Battlefield for Urban Operations*, RAND, Santa Monica, 2002.

Medina, Carmen, The Coming Revolution in Intelligence Analysis: What To Do When Traditional Models Fail, *Studies in Intelligence*, Central Intelligence Agency, Vol.46, No. 3, 2002, pp.23-28.

Meigs, Montgomery, Unorthodox thoughts about asymmetric warfare, *Parameters*, Vol.33, No.2, Summer 2003, pp.4-18.

Metcalf, Andrew, *Australia's National Security Preparedness - Where Next?*, presentation to Security in Government Conference 2005, Attonery-General's Department.

Montevideo Convention, 26 December 1933, accessed on 28 January 2010 at: http://avalon.law.yale.edu/20th_century/intam03.asp

Motley, James, International Terrorism: A Challenge for U.S. Intelligence, *International Journal of Intelligence and CounterIntelligence*, Spring 1986, pp.83-96.

Mueller, John, Is There Still a Terrorist Threat?, *Foreign Affairs*, Vol.85, No.5, Sep/Oct 2006, pp.2-8.

Muir, Angus, Trends in the Development of Terrorist Bombing, in (Ed.) Jones, David, *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004, p.80.

Müller-Wille, Björn *Thinking security in Europe - Is there a European Security and Defence Identity?*, Münster, 2003, (PhD Thesis), accessed on 28 July 2009 at: http://miami.uni-muenster.de/servlets/DerivateServlet/Derivate-1501/dissertation.pdf

Nacos, Brigette, The Terrorist Calculus behind 9-11: A Model for Future Terrorism?, *Studies in Conflict and Terrorism*, Vol.26, 2003, pp.1-16.

Naftali, *Blind Spot: The Secret History of American Counterterrorism*, Basic Books, New York, 2005.

Nye, Joseph, Peering into the Future, *Foreign Affairs*, July/August 1994, pp.82-93.

Nye, Joseph, *Soft Power: The Means to Success in World Politics*, PublicAffairs, New York, 2004.

Oakden, Edward, UK puts long-term perspective on countering terror attacks, *RUSI/Jane's Homeland Security and Resilience Monitor*, 01 June 2005, accessed on 26 July 2006 at: www.janes.com/

O'Brien, Kevin, Intelligence Gathering on Asymmetric Threats - Part One, *Jane's Intelligence Review*, Vol. 12, No.10, October 2000, pp.50-55.

O'Brien, Kevin, Information Age Terrorism and Warfare, in (Ed.) David Jones, *Globalisation and the New Terror: The Asia Pacific Dimension*, Edward Elgar, Cheltenham, 2004.

O'Day, Alan (Ed.), *Weapons of Mass Destruction and Terrorism*, Ashgate, Aldershot, 2004.

O'Day, Alan (Ed.), *Dimensions of Terrorism*, Ashgate, Aldershot, 2004.

Odom,William, Intelligence Analysis, *Intelligence and National Security*, Vol.23, No.3, pp.316-332.

O'halpin, Eunan, 'A poor thing but our own': The Joint Intelligence Committee and Ireland, 1965-72, *Intelligence and National Security*, Vol.23, No.5, October 2008, pp.658-680.

O'Neil, Andrew, Terrorist use of weapons of mass destruction: how serious is the threat?, *Australian Journal of International Affairs*, Vol.57, No.1, 2003, pp.99-112.

Ormand, Sir David, *The National Security Strategy: Implications for the UK intelligence community*, Institute for Public Policy Research, Discussion Paper, February 2009.

Palfy, Arpad, Weapon System Selection and Mass-Casualty Outcomes, *Terrorism and Political Violence*, Vol.15, No.2, Summer 2003, pp.81-95.

Patrick, Stewart, *Weak Links*: *Fragile States, Global Threats and International Security*, Oxford University Press, New York, 2011.

Paul, T.V., The National Security State and Global Terrorism: Why the State Is Not Prepared for the New Kind of War, in Ersel Aydinli and James Rosenau (Eds.), *Globilization, Security and the Nation-State: Paradigms in Transition*, State University of New York Press, Albany, 2005.

Perl, Matthew, Comparing US and UK Intelligence Assessment in the Early Cold War: NSC-68, April 1950, *Intelligence and National Security*, Vol.18, No.1, 2003, pp.119-154.

Pettiford, Lloyd; Harding, David, *Terrorism: The New World War*, Arcturus Publishing, Leicester, 2003.

Phillips, James, *The Evolving Al-Qaeda Threat*, Heritage Lectures No.928, The Heritage Foundation, 17 March 2006.

Phythian, Mark, Still a Matter of Trust: Post-9/11 British Intelligence and Political Culture, *International Journal of Intelligence and CounterIntelligence*, Vol.18, No.4, 2005, pp.653-681.

Phythian, Mark, Intelligence Analysis Today and Tomorrow', *Security Challenges*, Vol.5 No.1, Summer 2009, pp.69-85.

Pilch, Richard, The Bioterrorist Threat in the United States, in (Eds.) Russell Howard and Reid Sawyer, *Terrorism and Counterterrorism: Understanding the New Security Environment*, McGraw-Hill/Dushkin, Guilford, 2004.

Pillar, Paul, Intelligence, in Audrey Cronin and James Ludes (Eds.), *Attacking Terrorism: Elements of a Grand Strategy*, Georgetown University Press, Washington D.C., 2004.

Pollard, Neal, Globalization's Bastards: Illegitimate Non-State Actors in International Law in Bunker, Robert (Ed.), *Networks, Terrorism and Global Insurgency*, Routledge, London, 2005.

Pope, Simon; and Josang, Audun, *Analysis of Competing Hypotheses Using Subjective Logic*, Proceedings of the 10th International Command and Control Research and Technology Symposium, 2005.

Powers, Thomas, *Intelligence Wars: American Secret History from Hitler to al-Qaeda*, New York Review Books, New York, 2004.

Prillaman, William; Dempsey, Michael, Mything the Point: What's Wrong with the Conventional Wisdom about the C.I.A., *Intelligence and National Security*, Vol.19, No.1, Spring 2004, pp.1-28.

Prins, Gwyn, The four-stroke cycle in security studies, *International Studies*, Vol.74, No.4, 1998, pp.781-808.

Prober, Joshua, *Accounting for Terror: Debunking the Paradigm of Inexpensive Terrorism*, The Washington Institute for Near East Policy, Policy Watch No.1041, 1 November 2005, accessed on 2 July 2009 at: www.washingtoninstitute.org/

Prunkun, Hank, *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*, The Scarecrow Press, Lanham, 2010.

Quiggin, Thomas, *Seeing the Invisible: National Security Intelligence in an Uncertain Age*, World Scientific, Singapore, 2007.

Rabasa, Angel; Chalk, Peter; Cragin, Kim; Daly, Sara, Gregg, Heather; Karasik, Theodore; O'Brien, Kevin; Rosenau, William, Beyond al-Qaeda: The Global Jihadist Movement, RAND Corporation, Santa Monica, 2006.

Rasmussen, Mikkel, *The Risk Society at War: Terror, Technology and Strategy in the Twenty-First Century*, Cambridge University Press, Cambridge, 2006.

Raufer, Xavier, Al Qa'ida: A Different Diagnosis, *Studies in Conflict & Terrorism*, Vol.26, 2003, pp.391-398.

Realuyo, Celina; Stapelton, Scott, Response to Bali: An International success story, *eJournal Economic Perspectives*, US State Department, September 2004, accessed on 31 March 2009 at: http://usinfo.state.gov/

Reed, Brian, A Social Network Approach to Understanding an Insurgency, *Parameters*, Summer 2007, pp.19-30.

Reiber, Steven, Intelligence Analysis and Judmental Calibration, *International Journal of Intelligence and CounterIntelligence*, Vol.17, No.1, Spring 2004, pp.97-112.

Richelson, Jeffrey, *A Century of Spies: Intelligence in the Twentieth Century*, Oxford University Press, New York, 1995.

Richmond, Oliver, Realizing Hegemony? Symbolic Terrorism and the Roots of Conflicts, *Studies in Conflict & Terrorism*, Vol.26, 2003, pp.289-309.

Ried, Anna (Ed.), *Taming Terrorism: It's Been Done Before*, Policy Exchange, London, 2004.

Roberts, Nick, Defining 'Global Reach' Terrorism, *Defence Studies*, Vol.3, No.2, Summer 2003, pp.1-19.

Robinson, Paul, Why Britain Needs a New Defence Policy, *RUSI Journal*, Vol.150, No.4, August 2005, pp.32-35.

Rodin, David, Terrorism without Intention, *Ethics*, Vol.114, July 2004, pp.752-771.

Ronczkowski, Michael, *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations*, CRC Press, Boca Raton, 2004.

Rolington, Alfred, Keeping intelligence objective, *Jane's Intelligence Review*, 01 December 2005.

Rolington, Alfred, Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.738-759.

Roper, Daniel, *Transnational Threats: U.S. Military Strategy*, in Carolyn Pumphrey (Ed.), *Transnational Threats: Blending Law Enforcement and Military Strategy*, US Army War College, Strategic Studies Institute, November 2000, pp.41-49.

Ross, A.T., *Threat Recognition and Response*, Vol.1, Central Studies Establishment, Canberra, August 1986.

Ross, A.T., *Threat Recognition and Response*, Vol.2, Central Studies Establishment, Canberra, August 1986.

Rousseau, David, *Identifying Threats and Threatening Identities: The Social Construction of Realism and Liberalism*, Stanford University Press, Stanford, 2006.

Rovner, Joshua; Long, Austin, The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission, *International Journal of Intelligence and CounterIntelligence*, Vol.18, No.4, 2005, pp.609-637.

Rudner, Martin, Hunters and Gatherers: The Intelligence Coalition Against Islamic Terrorism, *International Journal of Intelligence and CounterIntelligence*, Vol.17, No.2, Summer 2004, pp.193-230.

Rumsfeld, Donald, Transforming the Military, *Foreign Affairs*, May/Jun 2002, Vol. 81,

Issue 3, pp.20-32.

Runge, Jeffrey, *Testimony of Jeffrey W. Runge, MD before the U.S. House of Representatives Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology*, accessed on 4 January 2010 at: www.dhs.gov/

Russell, Richard, Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities, in Loch Johnson (Ed.), *The Oxford handbook of national security intelligence*, Oxford University Press, Oxford, 2010.

Ryan, Maria, Filling in the 'Unknowns': Hypothesis-Based Intelligence and the Rumsfeld Commission, *Intelligence and National Security*, Vol.21, No.2, April 2006, pp.286-315.

Sageman, Marc, *Understanding Terror Networks*, University of Pennsylvania Press, Philadelphia, 2004.

Sageman, Marc, *Leaderless Jihad: Terror Networks in the Twenty-First Century*, University of Pennsylvania Press, Philadelphia, 2008.

Sageman, Marc; and Hoffman, Bruce, Does Osama Still Call the Shots? Debating the Containment of al Qaeda's Leadership, *Foreign Affairs*, Vol.87, 2008, pp.163-166.

Saikal, Amin, Afghanistan, terrorism, and American and Australian responses, *Australian Journal of International Affairs*, Vol.56, No.1, 2002, pp.23-30.

Salama, Sammy; and Hansell, Lydia, Does Intent equal Capability? Al-Qaeda and Weapons of Mass Destruction, *The Nonproliferation Review*, Vol.12, No.3, 2005, pp.615 – 653.

Scholz, J., *Vulnerability and a High-Tech Adaptive Society*, presentation to the 2nd International Policing Conference, Adelaide, November 2004, accessed on 31 March 2005 at: www.ipc2004.com/ (link no longer available).

Schreier, Fred, Transnational Terrorism: The Newest Mutation in the Forms of Warfare, in Winkler, Theodor; Ebnother, Anja; Hansson, Mats (Eds.), *Combating Terrorism and Its Implications for the Security Sector*, Swedish National Defence College, Stockholm, 2005, pp.45-57.

Scott, Len; Jackson, P.D. (Eds.), *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, Routledge, London, 2004.

Scott, Len; Jackson, Peter, The Study of Intelligence in Theory and Practice, *Intelligence and National Security*, Vol.19, No.2, Summer 2004, pp.139-169.

Scott, Len; Hughes, Gerald, Intelligence, Crises and Security: Lessons from History?, *Intelligence and National Security*, Vol.21, No.5, October 2006, pp.653-674.

Schulte, Paul, 'I am Osama bin Laden': A Strategic Warning and Challenge to the West, *RUSI Journal*, June 2002, pp.20-27.

Shultz, Richard; Godson, Roy, Intelligence Dominance: A better way forward in Iraq, *The Weekly Standard*, 31 July 2006, pp.22-26.

Schmid, Alex, Terrorism as Psychological Warfare, *Democracy and Security*, Vol.1, No.2, 2005, pp.137-146.

Schmitt, Gary, Truth to Power? Rethinking Intelligence Analysis, in ed. Peter Berkowitz, *The Future of American Intelligence*, Hoover Institution Press, Stanford, 2005.

Schneier, Bruce, *Why Data Mining Won't Stop Terror*, 09 March 2006 accessed on 11 March 2011 at: www.wired.com/

Schwien, Edwin, *Combat Intelligence: Its Acquisition and Transmission*, Washington, D.C., The Infantry Journal Inc., 1936.

Scott, Len, British Strategic Intelligence and the Cold War, in Loch Johnson (Ed.), *The Oxford handbook of national security intelligence*, Oxford University Press, Oxford, 2010.

Seebeck, Lesley, Cadence, war and security, *Australian Journal of International Affairs*, Vol. 58, No. 4, December 2004, pp. 494-510.

Segell, Glen, Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004, *International Journal of Intelligence and Counterintelligence*, Vol.18, No.2, pp.221-238.

Segell, Glen, Terrorism on London Public Transport, *Defence & Security Analysis*, Vol.22, No.1, March 2006, pp.45-59.

Segell, Glen, Three Intelligence Methodologies for Border Defence and Border Security, *Scientia Militaria*, Vol.33, No.2, 2005, pp. 1-23.

Sen, Amartya, *Rationality and Freedom*, The Belknap Press of Harvard University Press, Cambridge, 2002.

Sen, Amartya, *Identity and Violence: The Illusion of Destiny*, W.W. Norton and Company, New York, 2006.

Senechal de la Rocher, Roberta, Collective Violence as Social Control, *Sociological Forum*, Vol.11, No.1, March 1996, pp.97-128

Shukman, Harold (Ed.), *Agents for Change: Intelligence Services in the 21st Century*, St Ermin's Press, London, 2000.

Shulsky, Abram; Schmitt, Gary, *Silent Warfare: Understanding the World of Intelligence*, Third Edition, Brassey's, Washington, D.C., 2002.

Shultz, Richard; Farah, Douglas; and Lochard, Itamara, *Armed Groups: A Tier-One Security Priority*, INSS Occassional Paper No.57, Colorado, September 2004.

Shultz, Richard; Godson, Roy; and Quester, George, *Security Studies for the 21st Century*, Brassey's, Washington, 1997.

Sims, Jennifer, Intelligence to Counter Terror: The Importance of All-Source Fusion, in Loch Johnson (Ed.), *Strategic Intelligence 4: Counterintelligence and Counterterrorism: Defencing the nation against hostile forces*, Praeger Security International, Westport, 2007.

Sinai, Joshua, How to Forecast Intentions, Capabilities and Likelihood of Terrorist Groups Resorting to Low Impact Catastrophic Warfare, *Journal of Counterterrorism and Homeland Security International*, Vol.9, No.1, 2003, pp.19-22.

Sinai, Joshua, *How to Forecast and Preempt al-Qaeda's Catastrophic Terrorist Warfare*, accessed on 1 October 2004 at: http://www.homelandsecurity.org/

Singer, J. David, Threat Perception and the Armament-Tension Dilemma, *Journal of Conflict Resolution*, Vol.2, No.1, March 1958, pp.90-105.

Singer, J. David, Tensions, Political Settlement and Disarmament, in John Garnett (Ed.), *Theories of Peace and Security: A Reader in Contemporary Strategic Thought*, Macmillan, London, 1970.

Singer, J. David (Ed.), *The Correlates of War 1: Research Origins and Rationale*, The Free Press, New York, 1979.

Singer, J. David, Accounting for International War: The State of the Discipline, *Journal of Peace Research*, No.1, Vol.18, 1981, pp.1-18.

Skillicorn, David, *Knowledge Discovery for Counterterrorism and Law Enforcement*, Taylor and Francis, Boca Raton, 2009.

Sloan, Stephen, Foreword: Responding to the Threat, in (Ed.) Robert Bunker, *Networks, Terrorism and Global Insurgency*, Routledge, London, 2005.

Sloan, Elinor, *Security and Defence in the Terrorist Era: Canada and North America*, McGill-Queen's University Press, Montreal, 2005.

Smith, Andrew, Detecting Terrorist Activity: Defining the State's 'Threshold of Pain', *Australian Defence Force Journal*, No.168, 2005, pp.30-44.

Smith, Andrew, Preparation, Crisis and Consequence: Combating the New Threat of Mass-Casualty Terrorism, *Australian Army Journal*, Vol.1, No.1, pp.47-57.

Smith, Jacqui, '*Our shared values - a shared responsibility*' (First International Conference on Radicalisation and Political Violence in January 2008) accessed on 3 July 2009 at: http://press.homeoffice.gov.uk/Speeches/sp-hs-terrorism-keynote-jan-08

Smith, Rupert, *The Utility of Force: The Art of War in the Modern World*, Allen Lane, London, 2005.

Smith, Steve, The increasing insecurity of security studies: Conceptualizing security in the last twenty years, *Contemporary Security Policy*, Vol.20, No.3, December 1999, pp.72-101.

Snow, David, *National Security: Enduring Problems in a Changing Defense Environment*, 2nd Edition, St Martin's Press, New York, 1991.

Snowden, David, Complex acts of knowing – paradox and descriptive self-awareness, *Journal of Knowledge Management*, Spring 2002, accessed on 23 January 2007 at: http://www.kwork.org/Resources/snowden.pdf

Snyder, Glenn, *Deterrence and Defense: Toward A Theory of National Security*, Princeton University Press, Princeton, 1961.

Steele, Robert, *The New Craft of Intelligence: Achieving Asymmetric Advantage in the face of Nontraditional Threats*, Strategic Studies Institute, Carlisle, February 2002.

Steele, Robert, Crafting Intelligence in the Aftermath of Disaster, *International Journal of Intelligence and CounterIntelligence*, Vol.15, No.2, 2002, pp.161-178.

Stech, Frank *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of National Research, November 1979.

Steinberg, Alan, Threat Assessment Technology Development, in Dey, Anind; Kokinoc, Boicho; Leake, David; Turder, Roy (Eds.), *Modeling and Using Context*, 5th International and Interdisciplinary Conference: Context 2005 Proceedings, Springer, Berlin, 2005, pp.490-500.

Stratfor, *The Jihadist CBRN Threat*, 10 February 2010 accessed at: http://www.stratfor.com/weekly/20100210_jihadist_cbrn_threat?ip_auth_redirect=1 on 3 March 2011.

Stratfor, *Focused on the Trees, the CIA Missed the Soviet Forest's Fall*, Mar 12, 2001, accessed by subscription on 7 March 2006.

Stewart, Del, Analyzing Terrorism, *Military Intelligence Professional Bulletin*, Vol.28, No.1, Jan-Mar 2002, pp.15-20.

Sullivan, David, Professionalism and Australia's Security Intellectuals: Knowledge, Power, Responsibility, *Australian Journal of Political Science*, Vol.33, No.3, 1998, pp.421-440.

Sullivan, John, The Frontiers of Global Security Intelligence: Analytical Tradecraft and Education as Drivers for Intelligence Reform, *Small Wars Journal*, 2008, accessed on 3 March 2011 at: http://smallwarsjournal.com/

Sullivan, John; Terrorism, Crime and Private Armies, in Bunker, Robert (Ed.), *Networks, Terrorism and Global Insurgency*, Routledge, London, 2005.

Taylor, Stan; Goldman, David, Intelligence Reform: Will More Agencies, Money, and Personnel Help?, *Intelligence and National Security*, Vol.19, No.3, Autumn 2004, pp.416-435.

Teamy, Kyle; Sweet, Jonathan, Organizing Intelligence for Counterinsurgency, *Military Review*, Vol.86, No.5, September-October 2006, pp.24-29.

Teffera, Eyoel; Sadagopan, Geetha; and Nunes-Vaz, Rick, *Root causes of Terrorism - A Systems View*, Defence Science and Technology Organisation, Edinburgh, 2004.

Tellis, Ashley; Bially, Janice; Layne, Christopher; McPherson, Melissa, *Measuring National Power in the Postindustrial Age*, RAND Corporation, Santa Monica, 2000, p.133.

Tenner, Edward, The Shock of the Old, in Clarke, David (Ed.), *Technology and Terrorism*, Transaction Publishers, New Brunswick, 2004.

Thornton, Rod *Asymmetric Warfare: Threat and Response in the Twenty-First Century*, Polity Press, Cambridge, 2007.

Toffler, Alvin; Toffler Heidi, *War and anti-war*, Little, Brown and Company, New York, 1993.

Treverton, Gregory, Intelligence crisis, *Government Executive*, Vol.33, No.14, November 2001, pp.18-25.

Treverton, Gregory, *Reshaping National Intelligence for an Age of Information*, Cambridge University Press, Cambridge, 2003.

Treverton, Gregory, Terrorism, Intelligence and Law Enforcement: Learning the Right Lessons, *Intelligence and National Security*, Vol.18, No.4, Winter 2003, pp.121-140.

Treverton, Gregory, *Next Steps in Reshaping Intelligence*, RAND, Santa Monica, 2005.

Treverton, Gregory, *Emerging Threats to National Security*, Testimony presented to the House of Representatives Permanent Select Committee on Intelligence on February 2, 2005, RAND, Santa Monica, 2005.

Treverton, Gregory; Jones, Seth, *Measuring National Power*, Conference Proceedings, RAND, Santa Monica, 2005.

Treverton, Gregory; Gabbard, C, *Assessing the Tradecraft of Intelligence Analysis*, RAND, Santa Monica, 2008.

Treverton, Gregory, Addressing "Complexities" in Homeland Security, in Loch Johnson (Ed.), *The Oxford Handbook of National Security Intelligence*, Oxford University Press, Oxford, 2010.

Turbiville, Graham, Preface: Future Trends in Low Intensity Conflict, in Bunker, Robert (Ed.), *Networks, Terrorism and Global Insurgency*, Routledge, London, 2005.

Turner, Michael, Intelligence Reform and the Politics of Entrenchment, *International Journal of Intelligence and CounterIntelligence*, Vol.18, No.3, Fall 2005, pp.383-397.

United Nations, *First report of the Analytical Support and Sanctions Monitoring Team*

appointed pursuant to resolution 1526 (2004) concerning Al-Qaida and the Taliban and associated individuals and entities, S/2004/679, 25 August 2004 accessed on 9 July 2009 at: http://www.un.org/Docs/journal/asp/ws.asp?m=S/2004/679

Van Creveld, Martin, *Technology and War: From 2000 B.C. to the Present*, Brassey's, London, 1991.

Vitug, Marites, From Madrid to Manila: Aspects of Terrorism in South-East Asia, in Hopkins, Scott (Ed.), *Asymmetry and Complexity: Selected papers from the 2005 Rowell Seminar and the 2005 Chief of Army's Conference*, Land Warfare Study Centre, Canberra, February 2007, pp.35-46.

Volti, Rudi, *Society and Technological Change*, 5th Edition, Worth Publishers, New York, 2006.

Von Clausewitz, Carl, *On War*, edited and translated by Michael Howard and Peter Paret, Princeton University Press, Princeton, 1984.

Waltz, Edward, *Knowledge Management in the Intelligence Enterprise*, Artech House, Boston, 2003.

Ward, Stephen, Evolution Beats Revolution in Analysis, Counterpoint to Carmen Medina's "The Coming Revolution in Intelligence Analysis", *Studies in Intelligence*, Central Intelligence Agency, Vol.46, No. 3, 2002, pp.29-36.

Warner, Michael (Ed.), *Central Intelligence: Origin and Evolution*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C., 2001.

Warner, Michael, Wanted: A Definition of "Intelligence", *Studies in Intelligence*, Central Intelligence Agency, Vol.46, No. 3, 2002, pp.15-22.

Wastell, Colin; Clark,Graeme; and Duncan, Piers, Effective Intelligence Analysis: The Human Dimension, *Journal of Policing, Intelligence and Counter Terrorism*, Vol.1, October 2006, pp.36-52.

Westin, Cary, *A Flawed National Blueprint to Homeland Security Reform: Right Idea, Wrong Approach*, U.S. Army War College, Carlisle, March 2006.

Whaley, Barton, *Stratagem: Deception and Surprise in War*, Artech House, Boston, 2007.

Williams, Clive; Taylor, Brendan, *Countering Terror: New Directions Post '911'*, Strategic and Defence Studies Centre, Canberra, 2003.

Williams, Clive, Australian security policy, post-11 September, *Australian Journal of International Affairs*, Vol.56, No.1, 2002, pp.13-21.

Willis, Henry; Morral, Andrew; Kelly, Terrence; Medby, Jamison, *Estimating Terrorism Risk*, RAND, Santa Monica, 2005.

Wing, Ian, *Refocusing Concepts of Security: The Convergence of Military and Non-military Tasks*, Land Warfare Studies Centre, Canberra, Working Paper No. 111, 2000.

Wing, Ian, Chaos Theory and Intelligence Analysis, *Australian Defence Force Journal*, No.115, November/December 2005, pp.21-26.

Wirtz, James, Counter-terrorism via Counter-proliferation, *Terrorism and Political Violence*, Vol.14, No.3, Autumn 2002, pp.129-140.

Wohlstetter, Roberta, *Pearl Harbour: Warning and Decision*, Stanford University Press, 1962.

Wolf, John, *Antiterrorist Initiatives*, Plenum Press, New York, 1989.

Wolfberg, Adrian, Full-Spectrum Analysis: A New Way of Thinking for a New World, *Military Review*, July-August 2006, pp.35-42.

Wolfberg, Adrian, *Investing in the Social Capital of Knowledge*, Proceedings of the 2005 International Conference on Intelligence Analysis, May 2005, accessed at: http://analysis.mitre.org/proceedings/Final_Papers_Files/20_Camera_Ready_Paper.pdf

Wolfendale, Jessica, Terrorism, Security, and the Threat of Counterterrorism, *Studies in Conflict & Terrorism*, Vol.30, 2007, pp.75-92.

Zegart, Amy, Cloaks, Daggers, and Ivory Towers: Why Academics Don't Study U.S. Intelligence, in Loch Johnson (Ed.), *Strategic Intelligence 1: Understanding the Hidden Side of Government*, Praeger Security International, Westport, 2007.

Zeytoonian, Dan, Intelligent Design: COIN Operations amd Intelligence Collection and Analysis, *Military Review*, Vol. 86, No.5, September-October 2006, pp.188-195.

Zimbardo, Philip, *The Lucifer Effect*, Random House, New York, 2007.

Zimmermann, Doron, Terrorism Transformed: The "New Terrorism," Impact Scalability, and the Dynamic of Reciprocal Threat Perception, *The Quarterly Journal*, Vol. 3, No. 1, March 2004, pp.19-39.

Zlotnick, Jack, Bayes' Theorem For Intelligence Analysis, Westerfield, H, (Ed.), *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal* Yale University Press, New Haven, 1995 accessed on 17 July 2007 at: www.cia.gov/

Zuhur, Sherifa, *A Hundred Osamas: Islamist Threats and the Future of Counterinsurgency*, Strategic Studies Institute, Carslile, December 2005.

Government Publications

Australia

Australian National Audit Office, *Commonwealth Agencies' Security Preparations for the Sydney 2000 Olympic Games*, Commonwealth of Australia, Canberra, August 1998.

Australian Security Intelligence Organisation, *ASIO Report to Parliament 2002-2003*, Commonwealth of Australia, Canberra, 2003.

Australian Security Intelligence Organisation, *ASIO Report to Parliament 2003-2004*, Commonwealth of Australia, Canberra, 2004.

Australian Security Intelligence Organisation, *ASIO Report to Parliament 2007-2008*, Commonwealth of Australia, Canberra, 2008.

Australian Security Intelligence Organisation, *ASIO Report to Parliament 2008-2009*, Commonwealth of Australia, Canberra, 2009.

Commonwealth Government, *Australian Defence*, Defence White Paper, Canberra, November 1976.

Commonwealth Government of Australia, *The Australian Intelligence Community: Agencies, functions, accountability and oversight*, Commonwealth of Australia, Canberra, 2006.

Department of Defence, *Australia's Strategic Planning in the 1990s*, Departmental Publications, Canberra, September 1989.

Department of Defence, *Future Warfighting Concept*, Commonwealth of Australia, Canberra, 2002.

Department of Defence, *Complex Warfighting*, Commonwealth of Australia, Canberra, April 2004.

Department of Defence, *Australia's National Security: Defence Update 2003*, Commonwealth of Australia, Canberra, 2003.

Department of Defence, *Australia's National Security: Defence Update 2007*, Commonwealth of Australia, Canberra, 2007.

Department of Defence, *Joint Operations for the 21st Century*, Commonwealth of Australia, Canberra, 2007.

Department of Defence, *Defending Australia in the Asia Pacific Century: Force 2030*, Commonwealth of Australia, Canberra, 2009.

Department of Foreign Affairs and Trade, *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra, 2004.

Department of Prime Minister and Cabinet, *Protecting Australia Against Terrorism*,

Commonwealth of Australia, Canberra, 2004.

Dibb, Paul, *Review of Australia's Defence Capabilities*, Report to the Minister for Defence, March 1986.

Hill, Robert, *The Changing Security Environment*, Speech, 24 January 2004.

Hill, Robert, *Regional Terrorism, Global Security and the Defence of Australia*, speech to RUSI Triennial International Seminar National Convention Centre, Canberra, 9 October 2003.

Rudd, Kevin, *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia, 4 December 2008.

Varghese, Peter, *Australia's Strategic Outlook: A Longer-Term View*, Speech by the Director-General of the Office of National Assessments to the Australian Strategic Policy Institute, Canberra, 28 June 2006.

Canada

Criminal Intelligence Service Canada, Strategic Early Warning for Criminal Intelligence: Theoretical Framework and Sentinel Methodology, Central Bureau, Ottawa, 2007.

Singapore

Ministry of Home Affairs, *White Paper: The Jemaah Islamiyah arrests and the threat of terrorism*, Ministry of Home Affairs Republic of Singapore, 7 January 2003.

United Kingdom

10 Downing Street, *Responsibility for the Terrorist Atrocities in the United States: 11 September 2001*, 4 October 2001.

10 Downing Street, *Responsibility for the Terrorist Atrocities in the United States: 11 September 2001- An Updated Account*, 14 October 2001.

Cabinet Office, *The United Kingdom and The Campaign against International Terrorism: Progress Report*, 9th September 2002.

Cabinet Office, *National Intelligence Machinery*, The Stationery Office, London, November 2006.

Cabinet Office, *The National Strategy of the United Kingdom: Security in an interdependent world*, The Stationery Office, London, March 2008.

Cabinet Office, *The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation*, The Stationery Office, London, June 2009.

Crown Prosecution Service, Counter-Terrorism Division, accessed 9 July 2009 at: http://www.cps.gov.uk/publications/prosecution/ctd.html

Intelligence and Security Committee, *Intelligence Oversight*, The Stationery Office, London, 2002.

Intelligence and Security Committee, *Annual Report 2003–2004*, The Stationery Report, London, 2004.

Intelligence and Security Committee, *Annual Report 2004–2005*, The Stationery Office, 2005.

Intelligence and Security Committee, *Intelligence and Security Committee: Annual Report: 2006-2007*, The Stationery Office, London, 2008.

Intelligence and Security Committee, *Intelligence and Security Committee: Annual Report 2004–2005*, The Stationery Office, London, 2005.

Ministry of Defence, *Strategic Defence Review*, The Stationery Office, London, July 1998.

Ministry of Defence, *Delivering Security in a Changing World*, The Stationery Office, London, 2003.

Ministry of Defence, Future Character of Conflict, *Development Concepts and Doctrine Centre*, Shrivenham, 2010.

Operation CREVICE, accessed 09 July 2009 at:
http://www.mi5.gov.uk/output/terrorist-trial-convictions.html.

United Kingdom Government, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, The Stationery Office, London, October 2010.

United Kingdom Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, The Stationery Office, London, October 2010.

United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2006.

United Kingdom Government, *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009.

United States of America

Bush, George W., *National Security Strategy of the United States of America*, The White House, Washington, D.C., September 2002.

Bush, George W., *The National Security Strategy of the United States of America*, The White House, Washington, D.C., March 2006.

Department of the Army, *Field Manual 34-130 Intelligence Preparation of the Battlefield*, Washington, D.C., 1994.

Department of Defense, *Quadrennial Defense Review Report*, Washington, D.C., September 2001.

Department of Defense, The National Defense Strategy of The United States of America, Washington, D.C., March 2005.

Department of Defense, *Quadrennial Defense Review Report*, Washinton, D.C., February 2010.

Director of Central Intelligence, *A Consumer's Guide to Intelligence*, Diane Publishing Company, March 1999.

Department of Homeland Security, accessed on 21 November 2009 at: http://www.dhs.gov/xabout/strategicplan/.

Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, Washington, D.C., February 2010.

Federal Bureau of Investigation definition of WMD, accessed on 10 July 2009 at: http://www.fbi.gov/hq/nsb/wmd/wmd_definition.htm

Federal Bureau of Investigation, *Intelligence Philosophy*, accessed 13 October 2009 at: www.fbi.gov/intelligence/philio.htm.

Joint Chiefs of Staff, *The National Military Strategy of the United States of America, A Strategy for Today; A Vision for Tomorrow*, Washington, D.C., 2004.

Joint Chiefs of Staff, *Joint and National Intelligence Support to Military Operations*, Joint Publication JP 2-01, October 2004.

Joint Chiefs of Staff, *Joint Intelligence Preparation of the Operational Environment*, Joint Publication 2-01.3, Washington, D.C., 16 June 2009.

National Security Council, *A National Security Strategy for a New Century*, White House, Washington, D.C., December 1999.

National Security Council, *National Strategy for Combating Terrorism*, Washington, D.C., February 2003.

National Security Council, *National Strategy for Combating Terrorism*, Washington, D.C., September 2006.

Obama, Barack, *National Security Strategy of the United States of America*, The White House, Washington, D.C., May 2010.

Office of the Assistant Secretary for Public Affairs, *Facing the Future: Meeting the Threats and Challenges of the 21st Century, Highlights of the Priorities, Initiatives, and Accomplishments of the U.S. Department of Defense 2001-2004*, Department of Defense, February 2005.

Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005.

Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005.

Office of the Director of National Intelligence, *National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation*, Washington, D.C., October 2005.

Office of Homeland Security, *National Strategy for Homeland Security*, Washington, D.C., July 2002.

Office of the Inspector General, *A Review of the Federal Bureau of Investigation's Counterterrorism Program: Threat Assessment, Strategic Planning, and Resource Management*, Report No.02-38, September 2002, accessed on 7 June 2007 at: www.usdog.gov/

Office of the National Counterintelligence Executive, *The National Counterintelligence Strategy of the United States of America*, Washington, D.C., 2007.

Office of the Under Secretary of Defense for Intelligence, *Defense Intelligence Strategy*, Washington, D.C., 2008.

United States Army, *A Military Guide to Terrorism in the Twenty-First Century*, US Army Training and Doctrine Command, Fort Leavenworth, 15 August 2007.

United States Nuclear Regulatory Authority, *Fact Sheet: Dirty Bombs*, March 2003 at: http://www.nrc.gov/reading-rm/doc-collections/fact-sheets/dirty-bombs-bg.html

White House, *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, Washington, D.C., October 2007.

White House, *National Security Strategy*, The White House, Washington, D.C., May 2010.

Declassified Intelligence Analysis

Australia

Defence Committee, *A Strategic Basis of Australian Defence Policy*, Defence Committee Report, 8 January 1953.

Joint Intelligence Committee, *Intelligence Aspects of the Strategic Basis for Australian Defence Policy*, JIC (M) Appreciation No.35/1956, August 1956.

Defence Committee, *Strategic Basis of Australian Defence Policy*, December 1958.

Defence Committee *Strategic Basis of Australian Defence Policy*, 5 March 1971.

Defence Committee *Strategic Basis of Australian Defence Policy*, 1 June 1973.

Defence Committee *Strategic Basis of Australian Defence Policy*, 3 October 1975.

United Kingdom
Committee of Imperial Defence, *The Military Situation in Germany,* CID Paper 926B, 11 December 1928.

Joint Intelligence Committee, *Russia's Strategic Interests and Intentions*, JIC (46) 1, London PRO, CAB 81/132, 1 March 1946.

Joint Intelligence Committee, *Soviet Interests, Intentions and Capabilities -General*, JI (47) 7/2 Final, 6 August 1947.

Joint Intelligence Committee, *The Soviet Threat*, JIC (51) 6, London PRO, CAB 158/12, 19 Jan 1951.

United States of America
Central Intelligence Agency, *Possibility of Direct Soviet Military Action During 1948*, ORE 22-48, 2 April 1948.

Central Intelligence Agency, *Estimate of the Effects of the Soviet Possession of the Atomic Bomb upon the Security of the United States and upon the Probabilities of Direct Soviet Military Action*, ORE 91-49, 6 April 1950.

Central Intelligence Agency, *Soviet Capabilities and Intentions*, National Intelligence Estimate NIE-3, 15 November 1950.

Central Intelligence Agency, *Soviet Foreign Policy in the light of the Summit Conference*, National Intelligence Estimate 11-13-55, November 1955, accessed on 12 February 2010 at: http://www.foia.cia.gov/.

Central Intelligence Agency, *Soviet Short-Term Intentions Regarding Berlin and Germany*, National Intelligence Estimate 11-7-61, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Director of Central Intelligence, *Communist Objectives, Capabilities, and Intentions in Southeast Asia*, NIE 10-62, 21 February 1962, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Central Intelligence Agency, *Soviet Military Capabilities and Policies, 1962-1967*, NIE-11-4-63, March 1963, available at CIA FOIA website http://www.foia.cia.gov/ accessed on 12 February 2010.

Central Intelligence Agency, *Intelligence Aspects of the "Missile Gap"*, November 1968, Declassified, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Central Intelligence Agency, *The Balance of Forces in Central Europe*, August 1977, Declassified, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Central Intelligence Agency, *The Soviet Challenge to US Security Interests*, National Intelligence Estimate 11/4-82, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Central Intelligence Agency, *Warning of War in Europe*, June 1984, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Director of Central Intelligence, *The Soviet Atomic Energy Program*, National Intelligence Estimate 11-2A-63, 2 July 1963, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Directorate of Intelligence, *Soviet Spending for Defense: Trends Since 1951 and Prospects for the 1980s*, November 1981, accessed on 12 February 2010 at: http://www.foia.cia.gov/

Donovan, William, *Letter to Mr James C. Dunn from William J. Donovan Re Question of Post-War Intelligence*, 27 November 1944.

National Intelligence Council, *Iraqi Military Capabilities Through 2003*, NIE 94-19, July 1994, accessed on 12 February 2010 at: http://www.foia.cia.gov/

National Intelligence Council, *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007.

National Intelligence Council, *The Terrorist Threat to the US Homeland*, Office of the Director of National Intelligence, Washington, D.C., July 2007.

National Intelligence Council, *Iraqi Military Capabilities Through 2003*, NIE 94-19, July 1994, accessed on 12 February 2010 at: http://www.foia.cia.gov/

National Security Council, *NSC-68: United States Objectives and Programs for National Security*, 14 April 1950.

Government Threat Levels

Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A, accessed at: www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub02.pdf

United Kingdom Government, *Threat Levels: The System to Assess the Threat from International Terrorism*, The Stationery Office, London, July 2006.

The United States Government has not publicly released the criteria used to establish national terrorism threat levels (Homeland Security Advisory System). The Threat Level System is described at: www.dhs.gov/xinfoshare/programs/Copy_of_press_release_0046.shtm

Testimony - Intelligence Officials

Freeh, Louis, Former Director, Federal Bureau of Investigation, testimony to *The Joint Inquiry on Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, 08 October 2002.

Jacoby, Lowell, Director, Defense Intelligence Agency, Joint Chiefs of Staff, written submission to *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*.

Kelly, Henry, Testimony to the Senate Committee on Foreign Relations, 6 March 2002, available at: http://www.fas.org/ssp/docs/kelly_testimony_030602.pdf accessed on 5 July 2009.

McConnell, Mike, Director of National Intelligence (DNI), testimony to the Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007.

Mueller, Robert, *Testimony of Robert S. Mueller, III, Director, FBI, Before the Select Committee on Intelligence of the United States Senate February 11, 2003,* accessed 10 July 2009 at: http://www.fbi.gov/

Mueller, Robert, *Statement Before the Select Committee on Intelligence of the United States Senate*, accessed on 7 June 2007 at: www.fbi.gov/

Mueller, Robert, *Globalization and Evolution of the Terrorist Threat,* Remarks Prepared for Delivery by Robert S. Mueller, III Director, Federal Bureau of Investigation, Council of Foreign Relations Washington, D.C. Febraury 23, 2009, accessed 10 July 2009 at: http://www.fbi.gov/

Tenet, George, *Worldwide Threat 2001: National Security in a Changing World*, Statement by Director of Central Intelligence George J. Tenet before the Senate Select Committee on Intelligence, 7 February 2001, accessed on 9 January 2006 at: www.cai.gov/

Woolsey, James, Testimony, 12 February 1998, U.S. House of Representatives Committee on National Security accessed on 31 March 2008 at: http://www.globalsecurity.org/intell/library/congress/1998_hr/h980212w.htm

US Joint Inquiry into the 11 September 2001 attacks

U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Report of *The Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, December 2002, at: http://www.gpoaccess.gov/serialset/creports/911.html.

Submissions

Armitage, Richard, *Testimony for Deputy Secretary of State Richard Armitage Hearing Before the Joint Intelligence Committee,* 19 September 2002.

Berger, Samuel, *Joint Intelligence Committee Testimony*, 19 September 2002.

Black, Cofer, *Testimony of Cofer Black*, 26 September 2002.

CIA Officer (unidentified), DCI Counterterrorist Center, *Statement for the Record SSCI/HPSCI Joint Inquiry Staff 9-11 Hearing*, 20 September 2002.

Clarke, Richard, testimony, 11 June 2002 to The Joint Inquiry into *Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*.

Fallis, Kie, *Statement for the Record: Lessons Learned and Actions Taken in Past Events,*

8 October 2001, accessed at: http://www.fas.org/irp/congress/2002_hr/100802fallis.pdf.

Freeh, Louis, *Statement of Louis Freeh, Former FBI Director, before the Joint Intelligence Committees*, 8 October 2002, accessed on 9 February 2010: http://www.fas.org/irp/congress/2002_hr/100802freeh.pdf.

Gilmore, James, *Testimony of James S. Gilmore, III Chairman, Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction before the Joint Hearing of the U.S. Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence on the Joint Inquiry into the September 11 Attacks*, 1 October 2002.

Hayden, Michael, *Statement for the Record by Lieutenant General Michael V. Hayden, USAF Director, National Security Agency/Chief, Central Security Service before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence*, 17 October 2002.

Hitz, Frederick, *Statement of Frederick P. Hitz, Lecturer of Public and International Affairs, Woodrow Wilson School, Princeton University, before the Joint Intelligence Committee of the U.S. Senate and U.S. House of Representatives investigating the events leading to the attacks of September 11, 2001*, 03 October 2002.

Jacoby, Lowell, *Statement for the Record for The Joint 9/11 Inquiry: Information Sharing of Terrorism-Related Data*, 1 October 2002, p.4, accessed on 11 February 2010 at: http://www.fas.org/irp/congress/2002_hr/100102jacoby.pdf

Jacoby, Lowell, *Statement for the Record for The Joint 9/11 Inquiry: DIA Response to Joint 9/11 Letter of Invitation*, Rear Admiral Lowell E. Jacoby, US Navy Acting Director, Defense Intelligence Agency, 17 October 2002.

Lake, Anthony, *Joint Intelligence Committee Testimony*, 19 September 2002.

Mueller, Robert, *Statement for the Record FBI Director Robert S. Mueller III Joint Intelligence Committee* Inquiry, 18 June 2002.

Mueller, Robert, *Testimony of Robert S. Mueller, III Director Federal Bureau of Investigation before the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence House of Representatives*, 17 October 2002.

Mueller, Robert, *Statement for the Record FBI Director Robert S. Mueller III Joint Intelligence Committee Inquiry*, 25 September 2002.

Pillar, Paul, *Statement of Paul R. Pillar to the Joint Inquiry of the Senate Select Committee on Intelligence and House Permanent Select Committee on Intelligence*, 8 October 2002.

Rolince, Michael, *Prepared Remarks of Michael E. Rolince before the Select Committee on Intelligence United States Senate and the House Permanent Select Committee on Intelligence House of Representatives*, 20 September 2002.

Taylor, Francis, *Testimony to the Joint Congressional Intelligence Committee Inquiry*

October 1, 2002 by Ambassador Francis X. Taylor Coordinator for Counterterrorism Department of State, 1 October 2002.

Tenet, George, *Final Draft 9-11 Testimony for the DCI Joint Inquiry Hearing*, 18 June 2002.

Tenet, George, *Written Statement for the Record of the Director of Central Intelligence Before the Joint Inquiry Committee*, 17 October 2002, accessed on 9 February 2010 at: http://www.fas.org/irp/congress/2002_hr/101702tenet.pdf.

Watson, Dale, *Statement for the Record of Dale L. Watson Executive Assistant Director Counterterrorism and Counterintelligence Federal Bureau of Investigation Before the Select Committee on Intelligence United States Senate and the Permanent Select Committee on Intelligence House of Representatives*, 26 September 2002.

White, Mary, *Statement of Mary Jo White Former United States Attorney for the Southern District of New York before the Joint Intelligence Committees*, 8 October 2002.

Wolfowitz, Paul, *Prepared Testimony of Deputy Secretary of Defense Paul Wolfowitz for the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence: Joint Inquiry Hearing on Counterterrorist Center Customer Perspective*, 19 September 2002.

Testimony

Declassified Transcript, Closed Hearing 11 June 2002, Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.

Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Hearings Before the Select Committee on Intelligence U.S. Senate and the Permanent Select Committee on Intelligence House of Representatives, Volume 2, October 1, 3, 8, and 17, 2002*, U.S. Government Printing Office, Washington, 2004.

Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001, *Hearings Before the Select Committee on Intelligence U.S. Senate and the Permanent Select Committee on Intelligence House of Representatives, Volume 1, September 18, 19, 20, 24 and 26, 2002*, U.S. Government Printing Office, Washington, 2004.

Inquiry Staff Reports

Hill, Eleanor, *Joint Inquiry Staff Statement, Part 1*, 18 September 2002, accessed 8 February 2010 at: http://www.fas.org/irp/congress/2002_hr/091802hill.html

Hill, Eleanor, *The Intelligence Community's Knowledge of the September 11 Hijackers Prior to September 11, 2001*, Joint Inquiry Staff Statement, 20 September 2002.

Hill, Eleanor, *The FBI's Handling of the Phoenix Electronic Communication and Investigation of Zacarias Moussaoui Prior to September 11, 2001*, Joint Inquiry Staff Statement, 24 September 2002.

Hill, Eleanor, *Counterterrorism Information Sharing with Other Federal Agencies and with State and Local Governments and the Private Sector*, Joint Inquiry Staff Statement, 1 October 2002.

Hill, Elanor, *Proposals for Reform within the Intelligence Community*, Joint Inquiry Staff Statement, 3 October 2002.

Hill, Eleanor, *Hearing on the Intelligence Community's Response to Past Terrorist Attacks Against the United States from February 1993 to September 2001*, Joint Inquiry Staff Statement, 8 October 2002.

Hill, Eleanor, *Joint Inquiry Staff Statement*, 17 October 2002.

Australian Senate Inquiry into the 10 October 2002 Bali Bombings

Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/report/e03.pdf.

Submissions

Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, Attachment A, accessed 16 June 2006 at: www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub02.pdf

Australian Security Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 19 June 2003, accessed 16 June 2006 at: http://www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/qon/asio.pdf

Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 28 May 2004, 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/qon/dio_qons.pdf.

Defence Intelligence Organisation, *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, 16 June 2006 at: http://www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/qon/defence.pdf

Office of National Assessments Submission, *Security threats to Australians in South-East Asia*, Submission No.3, 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub03.rtf.

Testimony

Transcript of 19 June 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 20 June 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 24 September 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 20 June 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 20 November 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 27 November 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 28 November 2003 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 28 May 2004 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 23 June 2004 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Transcript of 5 August 2004 Public Hearing, *Security threats to Australians in South-East Asia*, Official Committee Hansard accessed 16 June 2006 at: http://www.aph.gov.au/senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/

Investigations into the 7 July 2005 London Bombings

Home Office, *Report of the Official Account of the Bombings in London on 7th July 2005*, London, The Stationery Office, May 2006

Intelligence and Security Committee, *Intelligence & Security Committee: Report into the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2006.

Intelligence and Security Committee, *Could 7/7 Have Been Prevented?: Review of the Intelligence on the London Terrorist Attacks on 7 July 2005*, The Stationery Office, London, May 2009.

Additional Inquiries
Commission on the Roles and Capabilities of the US Intelligence Community, (Aspin-Brown Commission), *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*, accessed on 11 May 2009 at: http://www.gpoaccess.gov/int/index.html

National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report*, W.W. Norton & Company, New York, 2004.

Flood, Philip, *Report of the Inquiry into Australian Intelligence Agencies*, Commonwealth of Australia, Canberra, July 2004.

Graham, Bob; Talent, Jim; Allison, Graham; Cleveland, Robin; Rademaker, Steve; Roemer, Tim; Sherman, Wendy; Sokolski, Henry; Verma, Rich, *World At Risk:The Report of the Commission on the Prevention of WMD Proliferation and Terrorism*, Vintage books, New York, 2008.

Hearing of the Senate Committee on Homeland Security and Governmental Affairs, *Confronting the Terrorist Threat to the Homeland: Six Years After 9/11*, 10 September 2007.

Silberman, Laurence; and Robb, Charles, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*, United States Government Printing Office, Washington, D.C., March 2005.

Legislation
National Security Act of July 26, 1947, (as amended) accessed at: http://www.intelligence.gov/0-natsecact_1947.shtml on 11 April 2008.

Commonwealth of Australia, *Australian Security Intelligence Organisation Act 1979*, Act No. 113 of 1979 as amended.

Commonwealth of Australia, Intelligence Services Act 2001, Act No. 152 of 2001 as amended.

United Kingdom, *Intelligence Services Act 1994*.

News Articles
BBC, *London bombs cost just hundreds*, accessed on 9 July 2009 at: http://news.bbc.co.uk/2/hi/uk_news/4576346.stm

BBC, *Mumbai Attacks*, accessed 28 June 2010 at: http://news.bbc.co.uk/2/hi/in_depth/south_asia/2008/mumbai_attacks/default.stm

BBC, *21 July: Attacks, escapes and arrests*, accessed 5 July 2009 at: http://news.bbc.co.uk/2/hi/uk_news/6752991.stm

Independent Television News, *Court sees bomb effects*, accessed 9 July 2009 at: http://itn.co.uk/3967b7a45c8a1847f5ba6d060069a0ec.html

Kissane, Karen, *Tip-off led to intense 16-month investigation*, The Age, 17 September 2008, accessed 9 July 2009 at: http://www.theage.com.au/national/tipoff-led-to-intense-16month-investigation-20080916-4hxp.html?page=-1

Kirby, Terry, *London bomb suspect 'had come in contact with police three times'*, The Independent, accessed 9 July 2009 at: http://www.independent.co.uk/news/uk/crime/london-bomb-suspect-had-come-in-contact-with-police-three-times-432574.html

Public Broadcast Service, *Osama bin Laden v The U.S.: Edicts and Statements*, accessed 9 July 2009 at: http://www.pbs.org/wgbh/pages/frontline/shows/binladen/who/edicts.html

Bedi, Rahul, *Mumbai attacks: Indian suit against Google Earth over image use by terrorists*, The Telegraph, 9 December 2008, accessed on 28 June 2010 at: http://www.telegraph.co.uk/news/worldnews/asia/india/3691723/Mumbai-attacks-Indian-suit-against-Google-Earth-over-image-use-by-terrorists.html