1-1-2011

Intelligence analysis and threat assessment: towards a more comprehensive model of threat

Charles Vandepeer
Defence Science & Technology Organisation

DOI: 10.4225/75/57a02f17ac5ca
4th Australian Security and Intelligence Conference, Edith Cowan University, Perth Western Australia, 5th -7th December, 2011

INTELLIGENCE ANALYSIS AND THREAT ASSESSMENT: TOWARDS A MORE COMPREHENSIVE MODEL OF THREAT

Charles Vandepeer
Defence Science & Technology Organisation and University of Adelaide
charles.vandepeer@defence.gov.au

Abstract

A central focus of intelligence is the identification, analysis and assessment of threat. However, as acknowledged by intelligence practitioners, threat assessment lags behind the related field of risk assessment. This paper highlights how definitions of threat currently favoured by intelligence agencies are primarily based on threatening entities alone. Consequently, assessments of threat are almost singularly concerned with understanding an identified enemy's intentions and capabilities. This 'enemy-centric' approach to intelligence analysis has recently come in for criticism. In particular, the shortcomings of the current approach become apparent where the focus of intelligence analysis is on threats from difficult-to-identify sub-state or non-state actors. This paper argues that a model of threat singularly focussed on threatening entities overly simplifies what is an inherently complex, inter-related phenomenon between multiple entities. A more comprehensive taxonomy of threat is proposed which identifies various entities covered by the concept of threat. This taxonomy provides a starting point for developing a more rigorous approach to threat assessment which better reflects the complexity of the phenomenon of threat.

Keywords

Intelligence Analysis; Threat; Threat Assessment; Intentions; Capabilities; Environment; Risk; Referent; Threat Actor

'THREAT' IN INTELLIGENCE ANALYSIS

The analysis and assessment of threat constitute a primary focus of intelligence. This is evident from intelligence agencies' own statements, declassified analysis and the broader intelligence literature. Intelligence agencies themselves define their role in terms of a core focus on assessing and identifying threats. The Australian Security Intelligence Organisation (ASIO) self-defined role "is to identify and investigate threats to security, wherever they arise, and to provide advice to protect Australia, its people and its interests" (ASIO, 2011)

Similarly, according to their own website, the UK's Security Service (MI5) "is responsible for protecting the United Kingdom against threats to national security" (MI5, 2011). Declassified intelligence analysis reinforces the central importance and focus on threats within intelligence analysis. The establishment of formal intelligence agencies within the United Kingdom, United States and Australia further highlight the centrality of perceptions of threat. The establishment of Britain's Secret Service Bureau (forerunner to MI5 and MI6) in 1909 was as a response to fears over the possibility of a Germany invasion and espionage activities (Goodman, 2008). 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 Axis powers, and the perceived threat from the Soviet Union (Immerman, 2006). The US Department of Homeland Security emerged from the 11 September 2001 attacks, with similar concerns over terrorist attacks critical in the establishment of UK's Joint Terrorist Analysis Centre and Australia's National Terrorist Analysis Centre. Percy Cradock's observation on the UK's Joint Intelligence Committee (JIC) appears equally applicable to other intelligence agencies. Cradock notes JIC's "predilection for the threats rather than the opportunities" (Cradock, 2002). In his effort at defining intelligence, Ken Robertson highlights the centrality of threat to intelligence agencies, 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" (Robertson, 1987). Yet, despite this central focus on threat, the field of threat assessment appears to lag behind that of risk assessment.

Testimony by the Chief of Staff to the Director General of the Secret Service to the Coroner's Inquests into the London Bombings of 7 July 2005 provides a valuable insight into perceptions of threat assessment versus risk assessment within intelligence agencies. The Chief of Staff testified that:

> "…when we discuss "threat" where there is much less academic work going on than "risk", there is little academically-based training on threat assessment, that is much more based around our own

> experience, our experience of our partners, the police and others, and other foreign intelligence services and looking back on cases we've been involved in before" (MI5 Chief of Staff, 2011).

Even a quick review of the literature and academic research supports the assertion by MI5's Chief of Staff, with the apparent depth and rigour of the field of risk assessment compared with that of threat assessment. Additionally, where assessments of threat are based on personal experience, it is apparent how these can be subjective and less open to critique or review. One author who was researching threat assessment methodologies in the intelligence context noted that intelligence analysis often lacks transparency and replicablity when it comes to intelligence assessments. This is because it is difficult to determine how the results were obtained (i.e. lack of transparency) and the inability to repeat the study in order to check if similar results were possible. After all, these two factors - transparency and replicablity - form the core of the scientific method of inquiry which is what intelligence analysis is based (Prunckun, 2011).

This central focus on threat, more specifically a pre-occupation with threatening entities, has had unintentional consequences. Whilst a focus on threat actors appears logical, one limitation of the approach has been captured by Major General Michael Flynn, Captain Matt Pottinger, and Paul Batchelor in *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*. The report generated a great deal of attention as, at the time of publication, Major General Michael Flynn was the Deputy Chief of Staff, Intelligence (CJ2), for the International Security Assistance Force (ISAF) in Afghanistan. The use of "human terrain teams" can be seen as a response to this lack of knowledge. Indeed, the fact that these were required to be established can be seen as evidence in support of the argument by Flynn *et al.* that US intelligence was singularly focused on the enemy at the expense of understanding the broader socio-cultural environment. The report provided a critique of the performance of US intelligence in supporting counter insurgency (COIN) operations in Afghanistan. Flynn *et al.* argued that "because the United States has focused the overwhelming majority of collection efforts and analytical brainpower on insurgent groups, our intelligence apparatus still finds itself unable to answer fundamental questions about the environment in which we operate and the people we are trying to protect and persuade" (Flynn et al., 2010). Consequently, US intelligence's enemy-centric (or red-centric) focus led to an inability of analysts to be able to answer even the most basic questions about the Afghan population (Flynn et al., 2010). The term 'red' within the military and intelligence contexts is a generic reference to an enemy, with 'blue' referring to the 'friendly' force. According to Flynn *et al.*, there exists "a tendency to overemphasize detailed information about the enemy at the expense of political, economic, and cultural environment that supports it" (Flynn et al., 2010). This has hampered ISAF efforts within Afghanistan in limiting Commanders' understanding of the socio-cultural environment that their forces are attempting to influence. Even where the US intelligence has established broader approaches to threat assessment, these are still seen as a means of providing better analysis of an enemy. The Joint Intelligence Preparation of the Operating Environment (JIPOE) is an example of a US intelligence "macro-analytic approach" to assist in understanding an "operating environment". However, even this methodology reflects the enemy-centric perspective described by Flynn *et al.* As noted in the doctrine, JIPOE "provides a disciplined methodology for applying a holistic view of the operational environment to the analysis of adversary capability and intent" (Joint Chiefs of Staff, 2009).

Whilst Flynn *et al.* describe the problem within a military context, the default to enemy-centred analysis of threat is evident across intelligence analysis more broadly. For example, this 'red-centric' view of analysis is apparent in testimony by the then Director of ASIO to the Australian Senate inquiry into the 2002 Bali bombings. In response to the Committee's question over whether or not 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. …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 (Richardson, 2003).

Consequently, the 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" (Richardson, 2003). However, as noted by intelligence analysts themselves, intelligence agencies were never able to come to grips with understanding the identity or nature of Jemaah Islamiyah prior to the attacks (O'Malley, 2003). This 'red-centric' approach to intelligence analysis across counterinsurgency and counterterrorism operations is not surprising given that the model of threat widely accepted across intelligence agencies and the intelligence literature is based solely on assessments of *threatening* entities.

EPISTEMOLOGY OF THREAT

In this paper, epistemology is defined as the study of the nature of knowledge in a particular field. The epistemological problem considered here is how the concept of threat is understood within intelligence analysis. Across intelligence agencies and the intelligence literature, there is a remarkably consistent and dominant conceptual model of threat. This is captured by Richard Betts who argues that "[a] threat consists of capabilities multiplied by intentions; if either one is zero, the threat is zero" (Betts, 1998). The acceptance and use of this model is reflected in intelligence agencies' declassified formal threat levels and publications (UK Government, 2006, and ASIO, 2003). The widespread use of this approach supports Glen Segell's argument 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, and the primary methodology for military intelligence analysis (Segell, 2004). Consequently, the parameters of *intent* and *capability* can be described as the dominant episteme used to understand threat within the field of intelligence analysis. This paper 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 a 'red-centric' actor-based approach.

This dominant 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 against whom to assess intentions and capabilities. An insight into the fundamentals of an actor-based approach to threat assessment 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:

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 (Daase & Kessler, 2007).

When faced with difficult-to-identify threatening non-state actors, the debate has been over which parameter to focus attention on rather than a more comprehensive or robust model of threat (McConnell, 2007; Cooper, 2005; Dahl, 2005; Cordesman, 2002). 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. Nevertheless, as Segell notes, the intentions-capability methodology has not been particularly successful at the substate level as these do not involve an identifiable build-up of capability by state forces, nor political hierarchies whose intentions could be observed (Segell, 2004). Consequently, even with a singular focus on threatening non-state actors, difficulties in the ability to define and identify the nature and boundaries of these actors have not been overcome. In both counterinsurgency and counterterrorism, the difficulty in understanding the size and nature of threatening entities has remained. The argument that many of these are only part-time threat actors drawn into conflict also hampers accurate assessments of insurgent numbers and capabilities (Kilcullen, 2009).

In addition to *intent* and *capability*, other parameters which regularly appear within the literature include those of *vulnerability* and *opportunity*. Vulnerability is usually defined along the lines of susceptibility of a target to an attack (Pilch, 2004). Opportunity appears to relate to assessments of a space and time that exists outside or beyond both a threatened and threatening entity (Little & Rogova, 2006). Whilst these extensions arguably provide a more complex and 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 any model 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 remains ill-defined (as is often the case in counterinsurgency or counterterrorism), a greater number of parameters appears to increase rather than reduce the analytical complexities of threat assessment. Nevertheless, despite attempts at broadening the dominant episteme, the primary focus of assessments of threat remains primarily focussed on a threatening actor. This is evident in that when the parameters of vulnerability and opportunity are used, these are usually as *extensions* to the existing parameters, not replacements (Little & Rogova, 2006, Pilch, 2004, Steinberg, 2005, Vellani, 2007).

ONTOLOGY 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" (Müller-Wille, 2003). 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. Nonetheless, without an understanding of who or what is being threatened, attempts at assessing threat are potentially meaningless. Three basic, yet critical questions appear fundamental in identifying assumptions and framing assessments of threat:

- What is the type of threat being assessed? (i.e. military attack, espionage, economic sanctions, etc.);
- Who or what is the assessed threat against? (i.e. threatened actor or object); and
- Who is the threat from? (i.e. the threatening actor).

This paper argues that threat cannot be understood simply by focussing on a threatening actor, and that even assessments of a threatening actor's intentions and capabilities can only be understood against a defined referent. A simple, binary military example is useful for highlighting that threat is *relational* and is as much dependant upon who or what is *threatened* as to who or what is *threatening*. Figure 1 provides three examples (A, B, and C) to illustrate that any assessment of a threat posed by an enemy 'red' is in relation to the nature of 'blue'. This example admittedly provides a picture of a static, non-evolving enemy which does not here adapt in relation to Blue.

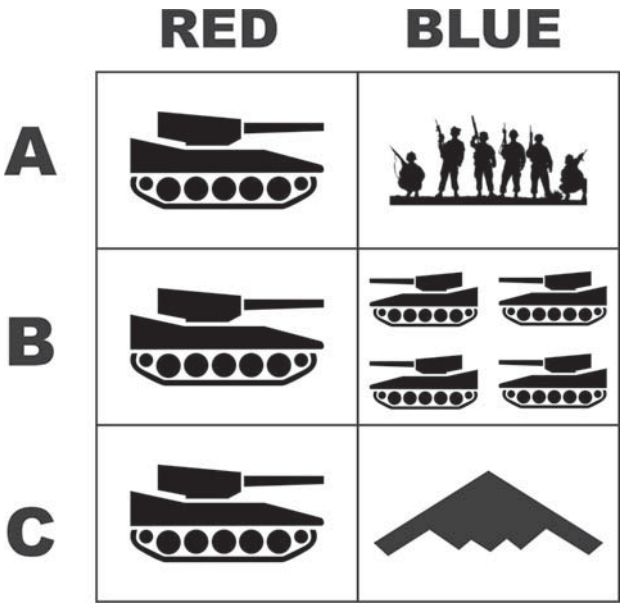

Figure 1. Relational Nature Of Threat: Red And Blue Entities

In a, an assessment of the threat posed by a single red tank is in relation to a group of blue soldiers. in b, red remains unchanged, but blue is changed to that of four tanks. in c, red remains unchanged, but blue is now an aerial bomber. in each of these, the assessed threat from red would be different. however, in each iteration, red remains the same, it is the blue column which changes, highlighting how threat is assessable only in relation to a defined threatened entity. this admittedly simple example demonstrates how the assessed level of threat changes irrespective of the lack of change in the threat actor. thus, intentions and capabilities of red are assessable only in relation to a defined entity; threat is as much a reflection of blue as red.

This paper defines ontology as the study of existence, and the nature and characteristics of entities. The ontological problem addressed here is defining the entities that constitute the concept of threat. Defining the nature of threatening and threatened entities provides an opportunity to consider a more comprehensive approach to understanding threat. 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

these states of affairs" (Little & Rogova, 2006). Rather than a formal ontology of threat, identifying the characteristics and nature of entities, this paper aims to provide a first step; developing a taxonomy of threat. This is an important initial step in critiquing the existing approach and moving towards a more comprehensive model that better reflects the complexity of the concept.

A potentially useful taxonomy used in describing *security* analysis is provided by Buzan, Waever and Wilde. They argue that 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) (Buzan et al., 1998).

This taxonomy can be adapted for intelligence analysis to describe the entities which make up threat. The entities defined in a taxonomy of threat are:

- a *referent* is what, or who, is threatened;
- a *threat actor* who is assessed by the *analyst* as threatening the *referent*;
- an *environment* within which threat actors and referents exist, emerge and evolve; and
- an *analyst* acts as a *'determiner of threat'* (equivalent to *securitizing actor*).

Having defined a taxonomy of threat, it is apparent that the conventional model of threat deals only with one entity: the threat actor. It is the threat actor's intentions and capabilities which form the basis for conventional approach to understanding threat and illustrate why analysts focus so heavily on threat actors at the expense of a more robust understanding of threat. A similar concept is discussed in Bill Flynt's paper *Threat Kingdom* in which Flynt develops a model of a security environment, including three elements: *threat, environment* and *self* (Flynt, 2000). Similarly, the JIPOE and Intelligence Preparation of the Battlespace (IPB) approaches consider the environment, but only towards establishing an assessment of a threat actor's intentions and capability. Additionally, 'blue' is not deliberately defined as part of a concept of threat within these approaches. As has been argued, threat is a much more complex phenomenon, involving inter-relations between different entities.

The traditional focus of security and defence has been about protecting the state from attacks by other states (Ormand, 2009). Within this context, the *referent* of threat was the state, specifically the survival of the state and its population. 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 (Ormand, 2009). 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" (Rudd, 2008).
- *The National Security Strategy* of the United Kingdom argues that "the security of our nation is the first duty of government", going on to state that the first core objective of the strategy is "ensuring a secure and resilient UK – protecting our people, economy, infrastructure, territory and way of life" (Cabinet Office, 2010).
- 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" (DHS, 2010).

The globalisation of state interests, due to increasing interconnectedness between states and non-state actors, and the movement of citizenry globally, makes clear identification of a state's interests, even population distribution, increasingly difficult. As noted earlier, however, meaningful assessments of threat require the identification and definition of a referent. Consequently, assessments of threat must deliberately define, rather than assume, the nature of the referent.

As discussed, the dominant approach to threat assessment currently favoured by intelligence agencies is on the intentions and capabilities of a threatening actor. Beyond this actor-based approach, there are alternative approaches for considering the threatening actors, particularly at the non-state level. As one example, is a *situationalist* approach to identifying the potential existence or emergence of threatening actors. This approach

considers factors external to individuals, acknowledging that violent behaviour is more likely to emerge under certain circumstances and situations (Zimbardo, 2007). This shifts assessment to the potential emergence of threatening actors prior to them having developed any hostile intentions or capabilities and provides an example of assessment beyond the current approach.

The concept of a *security* or *threat environment* is not new. However, the notion appears to have taken on an increased importance in efforts in grappling with the analytical and conceptual challenges presented by non-state threats. 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 (UK Government, 2009; Jenkins, 2006; DFAT, 2004). As evident in counterinsurgency operations where militaries are attempting to win 'hearts and minds', there is a recognised requirement to understand the socio-cultural environment of and in itself, as a critical factor in diminishing threat (Flynn et al., 2010).

The final actor defined in the taxonomy of threat is the *analyst*. The analyst is the individual who assesses both the threat actor and referent. Thus, how the analyst thinks and assesses threat is fundamental to understanding how judgements and decisions are made. Given that analysts are themselves making these decisions, this places them as critical actors within the process who have a substantial impact on how decision-makers perceive and act. In particular, it is the analyst who asks the questions which ultimately frame efforts at analysing and assessing threat.

CONCLUSION

The central focus on the identification and assessment of threat is apparent within intelligence analysis. Of note, the currently favoured model of threat is solely focussed on the intentions and capabilities of a defined threatening entity. However, this enemy-centric approach has been shown to have limitations particularly at the non-state and substate level. A simple analysis of the conventional approach highlights that even the intentions and capabilities of a threatening entity can only be assessed in relation to a threatened entity, highlighting that threat is a complex, inter-related phenomenon; a singular focus on the threat actor ignores this inter-relationship. Only after developing a taxonomy reflecting the complexity of threat can the nature and characteristics of these entities be explored and understood in order to inform assessments on threat. By describing an initial taxonomy of threat, this paper provides a first step in developing a more robust concept of threat that better reflects the complexity and relational nature of threat.

REFERENCES

ASIO website. (2011) Accessed on 12 October 2011 at: http://www.asio.gov.au/About-ASIO/Overview.html

ASIO. (2003) *Security threats to Australians in South-East Asia*, Submission No.2. Accessed on 16 June 2006 at: http://www.aph.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/submissions/sub02.pdf.

Betts, R. (1998) Intelligence Warning: Old Problems, New Agendas, *Parameters*, Spring, pp.26-35.

Buzan, B., Wæver, O. & de Wilde, J. (1998) *Security: A New Framework for Analysis*, Lynne Rienner Publishers, Boulder.

Cabinet Office. (2010) *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, The Stationery Office, London.

Christopher, D. & Kessler, O. (2007) Knowns and Unknowns in the 'War on Terror': Uncertainty and the Political Construction of Danger, *Security Dialogue*, Vol. 38, No. 4, pp. 411-434.

Cooper, J. (2005) *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, Centre for the Study of Intelligence, Central Intelligence Agency, Washington, D.C.

Cordesman, A. (2002) *Terrorism, Asymmetric Warfare, and Weapons of Mass Destruction: Defending the US Homeland*, Centre for Strategic and International Studies, Washington, D.C.

Cradock, P. (2002) *Know Your Enemy: How the Joint Intelligence Committee Saw the World*, John Murray, London.

Dahl, E. (2005) Warning of Terror: Explaining the Failure of Intelligence Against Terrorism, *The Journal of Strategic Studies*, Vol.28, No. 1, pp.31-55.

Department of Foreign Affair and Trade. (2004) *Transnational Terrorism: the threat to Australia*, Commonwealth of Australia, Canberra.

Department of Homeland Security. (2010) *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, Washington, D.C.

Flynn, Major General M., Matt Pottinger, Captain M. and Batchelor, P. (2010) *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Center for a New American Security.

Flynt, B. (2000) Threat Kingdom, *Military Review*, July-August, pp.12-21.

Goodman, M. (2008) Learning to Walk: The Origins of the UK's Joint Intelligence Committee, *International Journal of Intelligence and CounterIntelligence*, Vol.21, pp.40–56.

Immerman, R. (2006) A Brief History of the CIA in Theoharis, A., Immerman, R., Johnson, L., Kathryn, O. & Prados, J. (eds), *The Central Intelligence Agency: Security Under Scrutiny*, Greenwood Press, Westport.

Jenkins, B. (2006) *Unconquerable Nation: Knowing Our Enemy Strengthening Ourselves*, RAND Corporation, Santa Monica.

Joint Chiefs of Staff. (2009) *Joint Intelligence Preparation of the Operational Environment*, Joint Publication 2-01.3.

Kilcullen, D. (2009) *The Accidental Guerrilla: Fighting Small Wars in the Midst of a Big One*, Scribe, Melbourne.

Little, E. & Rogova, G. (2006) An Ontological Analysis of Threat and Vulnerability, in *Proceedings of the 9th International Conference on Information Fusion*, Center for Cognitive Science, Buffalo.

McConnell, M. (2007) 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*.

Müller-Wille, B. (2003) *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

O'Malley, W. (2003) Assistant Director-General, Southeast Asia Branch, Office of National Assessments, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003.

Ormand, D. (2009) *The National Security Strategy: Implications for the UK intelligence community*, Institute for Public Policy Research, Discussion Paper.

Pilch, R. (2004) 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.

Prunckun, H. (2011). Author's interview with Hank Prunckun author of *Handbook of Scientific Methods of Inquiry for Intelligence Analysis*.

Richardson, D. (2003) Director ASIO, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003.

Robertson, K. (1987) 'Intelligence, Terrorism and Civil Liberties', *Conflict Quarterly*, Vol.7, No.2, Spring, quoted in Herman, M (1996) *Intelligence power in peace and war*, Cambridge University Press, Cambridge.

Rudd, K. (2008) *The First National Security Statement to the Australian Parliament*, Address by the Prime Minister of Australia.

Security Service (MI5) website. (2011) Accessed on 12 October 2011 at: https://www.mi5.gov.uk/

Secret Service Chief of Staff. (2011) *Coroner's Inquests into the London Bombings of 7 July 2005*, Transcript of Testimony, 23 February 2011.

Segell, G. (2004) Intelligence Methodologies Applicable to the Madrid Train Bombings, *International Journal of Intelligence and Counterintelligence*, Vol.18, No.2, 2004, pp.221-238.

Steinberg, A. (2005) Threat Assessment Technology Development, in Dey, A., Kokinoc, B., Leake, D & Turder, R. (eds), *Modeling and Using Context*, 5th International and Interdisciplinary Conference: Context 2005 Proceedings, Springer, Berlin, pp.490-500.

United Kingdom Government. (2006) *Threat Levels: The System to Assess the Threat from International Terrorism*, The Stationery Office, London, July 2006, p.2.

United Kingdom Government. (2009) *The United Kingdom's Strategy for Countering International Terrorism*, Stationery Office, London, 2009.

Vellani, K. (2007) *Strategic Security Management: A Risk Assessment Guide for Decision Makers*, Elsevier, Oxford.

Zimbardo, P. (2007) *The Lucifer Effect*, Random House, New York.