

Intelligence Analysis as decision-making: A case study of the 2002 Bali Bombings

by

Charles Vandeeper

University of Adelaide

The views expressed in this paper reflect the author's personal judgments and do not necessarily represent the views of any department or agency of the Australian Government.

Abstract

This paper explores decision-making in intelligence analysis based on an examination of the Australian Senate Inquiry into the 2002 Bali bombings. The purpose is to draw lessons for decision-making and identify where current intelligence analysis approaches need to consider alternative concepts for decision-making about threats. The Inquiry provides a publicly accessible case study with which to critically examine how intelligence analysts identified, analysed and assessed terrorist threats in South East Asia prior to the 2002 Bali bombings. The testimony and submissions to the Inquiry makes it apparent that intelligence analysts make decisions on threat under conditions of uncertainty. Additionally, awareness of the existence of an organisation like JI does not provide analysts with everything they need to make sound decisions. Instead, intelligence analysts need concepts for decision-making about threats in the absence of specific information or knowledge of threats. This paper considers two potential approaches for judgements about threat that emerged during the Inquiry. The first approach is identifying factors indicating a potential for the unidentified existence or emergence of threats. The second approach is clearly defining national interests to specifically focus analytical efforts whilst drawing on information that is available.

Introduction

On 12 October 2002, members of the terrorist group *Jemaah Islamiyah* (JI)¹ detonated two bombs in Bali's tourist district causing the deaths of 202 people including 88 Australians and 24 British citizens. The bombers employed suicide as a tactic using bombs made up of commercial chemicals and TNT assembled on the island. Following the bombings, the Australian Senate Committee on Foreign Affairs and Defence conducted an inquiry to examine what Australian Government agencies knew about threats to Australian citizens in South East Asia in the lead up to the bombings. An inquiry into the attacks was also held in the United Kingdom, run by the Intelligence Security Committee. This paper focuses on the Australian Inquiry as it was the more comprehensive of the inquiries in terms of publicly released material. The UK's ISC report runs to 14 pages whereas the Australian Senate Inquiry, *Security threats to Australians in South East Asia*, conducted over fourteen months, publicly released around 600 pages of testimony and declassified intelligence assessments in addition to a nearly 200-page final report by the Committee. The reason for the

¹ Jemaah Islamiyah means 'Islamic Group' or 'Islamic Community'.

comprehensive public release of so much material perhaps reflects the surprise over the worst ever terrorist attack suffered by Australians either at home or overseas. That the attacks occurred in Bali was also unexpected. At the time, Bali was the most popular overseas tourist destination for Australians, and had been considered a safe destination for decades.

The Committee's final report observed that "important lessons have been learned from the tragic events of Bali" and hoped that their Final Report would "illuminate and extend those lessons"². It is in this spirit of considering what lessons can be drawn from these events that this paper is presented. Further, it is argued that the lessons drawn from the Australian Inquiry have applicability to Western intelligence analysis more generally. This paper does not focus on those who carried out the attack, there is already significant amounts of research into attempting to understand the motives and actions of individuals who conduct such attacks. Instead the focus of this paper is on the decisions analysts made about the threat and what lessons can be identified from an intelligence analysis perspective. Professor Christopher Andrew suggests four proven methodologies for learning from intelligence experience; lessons identified approach to significant events through case studies based on declassified intelligence; full-scale intelligence histories; retrospective analysis of assessments of the threat; and understanding how opponents assessed Western intelligence agencies³. This paper employs two of these methodologies, namely: lessons identified approach to the Bali bombings, and a retrospective analysis of assessments of threat.

Intelligence-analysis as decision-making

In attempting to define *intelligence*, the Committee highlighted Richard K. Betts' definition of strategic intelligence as "the acquisition, analysis and appreciation of relevant data"⁴ as being representative of definitions in the intelligence literature. Within the literature it is accepted that there is a difference between *information* and *intelligence*. Generally, the difference identified is that intelligence includes analysis of the information⁵. This definition focuses on human analysis or decision-making as the important distinction between the two concepts of information and intelligence. This paper employs the term *intelligence* to mean analysed information⁶. It is this

² The final report of the Senate Inquiry and all testimony and submissions referred to in this chapter are available at http://www.apf.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/index.htm (last accessed 20 June 2006)

³ Christopher Andrew, *Intelligence Analysis needs to look backwards before going forward*, accessed at www.historyandpolicy.org/papers/policy-paper-23.html

⁴ Richard K Betts 'Analysis, War and Decision: Why Intelligence Failures are Inevitable' in *World Politics* Princeton University Press (1978) p.61 quoted in Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.7

⁵ In testimony to the Inquiry, Professor Babbage noted the "difference between data, or pure information if you like, and intelligence. Intelligence is analysed and has judgment." Prof. Babbage, p.296 available at http://www.apf.gov.au/Senate/committee/fadt_ctte/completed_inquiries/2002-04/bali/index.htm (accessed 20 June 2006). Another argument in the literature focuses instead on the classified-nature of collected information defining this as intelligence. For example, the Australian Commonwealth Government defined intelligence as "covertly obtained information". The Australian Intelligence Community: Agencies, functions, accountability and oversight, Commonwealth of Australia 2006, p.3. Whilst information may be classified due to how it has been collected, this paper draws a distinction between information and intelligence based on the role of analysis.

⁶ During testimony and submissions provided to the Inquiry these two terms were used interchangeably which is reflected in some of the quotations used in this chapter.

analysis of information, and the judgements and assessments that analysts make about threat, which represents the fundamentally important decision-making process of intelligence analysis. As was evident in the Inquiry, the decisions analysts make directly influence the warnings issued to citizens travelling overseas. This paper focuses on the decisions analysts made leading up to the 2002 bombings, the reasoning and limitations behind such decisions and potential approaches for improving decision-making under conditions of uncertainty.

Australian Intelligence agencies

Analysts and officials from three Intelligence agencies to appear before the Inquiry into *Security threats to Australians in South East Asia*⁷ were the Australian Security Intelligence Organisation (ASIO), the Defence Intelligence Organisation (DIO) and the Office of National Assessments (ONA)⁸. Whilst these three groups form only part of the Australian Intelligence Community (AIC), they are the only intelligence agencies which conduct analysis and assessments on threats to Australia's national interests. In making decisions about threats, each of these agencies draw on all-source information, including intelligence, diplomatic reporting and open source material, such as news media, think-tank reports and academic publications⁹.

Jemaah Islamiyah

The Inquiry found that Australian intelligence agencies knew of the general threat of terrorism in South East Asia well before the 2002 Bali bombings. Further, the high priority given to identifying terrorist threats after the attacks of 11 September 2001 meant that Australian Intelligence agencies were looking for the types of threats posed by groups like JI¹⁰. Nevertheless, despite the general awareness of the threat of terrorism in South East Asia, intelligence agencies remained unaware of the existence of JI as a terrorist group¹¹, and possibly of the group's existence at all¹² until

⁷ Hereafter referred to as the Inquiry.

⁸ 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

⁹ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, Appendix 3

¹⁰ ONA, as coordinator for foreign intelligence collection: "...convened special meetings of collectors in the aftermath of 11 September 2001 to provide guidance on terrorism collection priorities. ...On Indonesia in particular, ONA convened in early 2001 a meeting to inform collectors of the higher priority ONA was giving to the assessment of radical Islam in Indonesia and its external links. ...In response, collection agencies made a concerted effort to increase coverage of Islamic extremists in the region." Submission by the Office of National Assessments, *Security threats to Australians in South-East Asia*, Submission No.3, p.4

¹¹ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xv.

¹² It is questionable whether the existence of JI was known to intelligence analysts prior to December 2001. The Inquiry did not appear to receive any evidence that Australian Intelligence agencies knew of the organisation at all before being informed by Singaporean authorities. An understanding of the

December 2001. It was only then that Singaporean authorities uncovered the existence of plans to conduct bombings against Western targets in Singapore that JI was identified¹³. The then Director-General of ASIO at the time testified to the Inquiry that:

The 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 2001¹⁴.

That is not to say that intelligence agencies were unaware a number of people who later turned out to be members of JI. The spiritual head of JI, Abu Bakir Bashiyar, was known to intelligence agencies as early as the mid-1980s as “a bomb thrower”¹⁵. However, the organisation Bashiyah led remained unidentified by these agencies. JI was able to escape the notice of Australian (and regional) intelligence agencies despite the high priority of counter-terrorism with intelligence collection efforts specifically aimed at collecting against the very type of threat that JI presented¹⁶. This lesson was not lost on one Australian research body, which concluded that “[g]iven that our intelligence agencies originally missed the development of JI [Jemaah Islamiyah] into a regional terrorist group with the intent and capability to threaten Australian interests there’s no guarantee that we could identify other emerging organisations.”¹⁷. This was not so much a criticism as a recognition of the difficulty of identifying such threats.

The short period between identification of JI and the Bali bombings represented a significant challenge for analysts. Intelligence agencies had (unknown to them) just ten months to establish an understanding of JI before the attacks in Bali. During these ten months analysts attempted to establish a history of JI, identify members of the group and assess the threat JI posed to Australian interests. However, developing an understanding of the network proved challenging.

Decisions about the threat prior to the Bali bombings

What the JI network was planning remained unclear to intelligence analysts up to the Bali bombings. According to DIO, the uncovering of the JI provided information on

group’s history appears to have been developed only after contact by the Singaporean authorities. This also appears to be the case for knowledge beyond the intelligence community. Whilst radical groups were known to exist in South East Asia, there does not appear to be a specific reference to Jemaah Islamiyah as an organisation prior to the release of the Singaporean White Paper on JI. This argument is supported by the Flood Inquiry, which found that until the Singaporean operation “[l]ittle was known about JI, under that name”. See Report into the Inquiry into Australian Intelligence Agencies [Flood Report], Phillip Flood AO, Commonwealth Government, Canberra, July 2004, p.36

¹³ One analyst acknowledged that “Until the Singaporean and Malaysian uncovering of Jemaah Islamiah, we knew very, very little” Mr Gordon, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 23 June 2004, p.524

¹⁴ Mr Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.3

¹⁵ Mr Gordon, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 23 June 2004, p.524

¹⁶ Mr Jones, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.125

¹⁷ Australian Strategic Policy Institute, *Local Jihad: Radical Islam and terrorism in Indonesia*, 2005, p.54

the group's potential targets, but did not make Bali stand out as one of these. A submission by DIO stated that "the evidence made public by Singapore indicated that external support would still have been required for terrorist attacks, which were planned against primarily official targets, such as embassies, armed forces units, military personnel off-duty, or ships."¹⁸ With no precedence for attacks in Bali¹⁹, and no information pointing to the planning for such an operation, analysts based their decisions on what they were able to collect on JI. The problem was that the JI network, or at least those members of the network responsible for the Bali attacks, behaved differently to the information collected. The threat to Australian interests in Indonesia was assessed by ASIO as High from December 2001 through to the Bali bombings and beyond. However, at no time was a threat assessment for Bali, or any other sub-region of Indonesia, issued by ASIO²⁰. So what decisions did intelligence analysts reach on the threat posed by JI prior to the Bali bombings?

At the time of the Bali bombings, intelligence agencies were attempting to develop an understanding of JI, but this remained limited, as seen by the final reports released by the Agencies prior to the 12 October bombings. Four days before the bombings, ASIO assessed that JI "may be planning attacks against Singaporean interests and assets throughout the Southeast Asian region"²¹. This assessment made no specific mention of a threat to Australia or Australian interests but assessed that "the possibility that Australian interests may be directly or indirectly affected by a regional campaign of violence by JI cannot be discounted."²² Less than one month out from 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."²³ Two days prior to the attacks, ONA released a report which provides insight into their understanding of the threat posed by JI:

...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. ...The

¹⁸ Defence Intelligence Organisation (Department of Defence), *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.3

¹⁹ Ronald Bonighton, Deputy Secretary, Intelligence and Security, Department of Defence, testified that "I do not think there had been any real terrorist action in Bali either. Certainly in the December 2000 bombings, which we found out later were done by JI, Bali was not one of the areas targeted, although there were a fair range of targets across Indonesia. So there was no form, no track record, of Bali being involved." Mr Bonighton, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.349

²⁰ This assessment influenced travel advisories issued by the Department of Foreign Affairs and Trade (DFAT) and influenced both DIO and ONA in their own judgements.

²¹ Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.5

²² Australian Security Intelligence Organisation Submission, *Security threats to Australians in South-East Asia*, Submission No.2, p.5

²³ Defence Intelligence Organisation (Department of Defence), *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.5

report also said key JI leaders, who have even bigger plans, including those who plotted the Singapore operation, are still free.²⁴

After the Bali bombings, the police investigation revealed the JI members involved in planning and conducting the attacks. Whilst several individuals involved in the attack were familiar to analysts, a number of those involved had never been identified²⁵. One analyst testified that his agency “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.”²⁶. The nature of JI itself was one of the main challenges that prevented analysts from accurately identifying preparations for the bombings.

The threat from networks, groups and cells

One of the issues which became apparent during the testimony is the difficulty in detecting the existence of these types of groups as well as the challenge of collecting information on these groups. That JI was a foreign-based group made identification and collection that much more difficult for Australian agencies, particularly when Indonesian authorities were not necessarily convinced of the threat²⁷. Unlike strategic intelligence during the Cold War in which nations, in particular their elites and militaries, tended to be the primary intelligence priority, major terrorist attacks against civilians have seen terrorist groups become a strategic priority for intelligence agencies²⁸. Nations, which draw international legitimacy from their visibility and clearly defined borders, are inherently visible collection targets. Groups such as JI, however, present themselves as very different threats which, because of their covert nature present a difficult intelligence target²⁹. The difficulty of detecting and collecting against JI was highlighted by agencies noting the challenge of “tightly knit, cell-based groups of carefully recruited militants, who combined modern telephon[e] and internet with traditional, direct word-of-mouth communications”³⁰. One observation was that JI members “look like ordinary people going about their everyday business”³¹

²⁴ Office of National Assessments Submission, *Security threats to Australians in South-East Asia*, Submission No.3, p.9

²⁵ It is interesting to note that similar conclusions emerged following the 11 September 2001 and July 2005 London bombings.

²⁶ Dr O’Malley, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.126

²⁷ The Committee’s final report observed that “Australia’s intelligence agencies did not know, before December 2001, of the existence of JI as a terrorist organisation. If there was any notable omission thereafter that contributed to the disaster it was 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.” Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xv

²⁸ The 2006 Government publication, *The Australian Intelligence Community: Agencies, functions, accountability and oversight*, the Australian Intelligence Community was described as “the front line in the fight against terrorism.”p.2

²⁹ Defence Intelligence Organisation (Department of Defence), *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.4

³⁰ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.105

³¹ Mr Bonighton, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353

In terms of specific information that would have been required for preventing the Bali bombings, the type of information required would have needed to come from within JI itself, which of course was very difficult to acquire³². Unlike the more conventional intelligence collection targets (such as countries), the JI network was not confined to well-defined political and geographic borders. Instead, JI was a regionally-based network with members in Singapore, Malaysia, Indonesia and the southern Philippines and linked more broadly to al Qa-eda³³. Intelligence agencies were faced with a transnational, covert and close-knit network that remained difficult to identify, collect against and accurately assess.

In search of specific information

Officials from each intelligence agency to appear before the Inquiry gave evidence of a lack of specific information indicating the planning for attacks in Bali. This assertion was supported by the Inspector General of Intelligence and Security, who testified 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.”³⁴ The issue of an ‘absence of information’ is worth exploring. The Committee found that the intelligence agencies “were carrying out analysis and delivering assessments that were optimal within the bounds of the information and evidence available to them.”³⁵. The Committee referred to testimony supporting this conclusion, which argued that:

We have to be realistic about what even a well-funded and very capable intelligence system can deliver. It is unrealistic to expect that our intelligence agencies can provide us, reliably and with great specificity, with warnings of terrorist attacks before they occur - for example, that an attack will occur on the following day at the following place.³⁶

The Bali bombings indicate that there is no guarantee that specific information that could warn of a specific attack *will* be collected or even *could* be collected. The bombings also indicate the scale of an operation that can go undetected.

Fortunately, the conclusion over the absence of specific information was not the end of the Committee’s analysis. The Chair of the Inquiry noted that a constant reference by officials and analysts to a lack of specific information “does not really advance the discussion very far”³⁷. The Committee concluded that “it seems self-evident - given JI’s previous history of avoiding detection and its almost family-like cell-based structure - that it would have been extremely unlikely that agencies would find

³² Dr Wright-Neville, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 November 2003, p.260

³³ Defence Intelligence Organisation (Department of Defence), *Security threats to Australians in South-East Asia*, Answers to Questions on Notice 20 June 2003, p.3

³⁴ Mr Blick, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.95

³⁵ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.27

³⁶ Mr White, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 27 November 2003, p.314

³⁷ Official Committee Hansard, *Security threats to Australians in South-East Asia*, Friday, 28 May 2004, p.452

themselves suddenly in possession of specific information about a JI terrorist attack in any particular place in Indonesia”³⁸. Intelligence analysts pursue specific intelligence, but almost invariably settle for less, yet are still required to make sound judgments³⁹. It is, therefore, consideration of approaches for making sound decisions about threats, in the absence of specific information, which this paper now considers.

Drawing lessons for decision-making about threats

It is evident from the Inquiry that analysts are unlikely to have all the information necessary to make sound or insightful decisions about threats from networks or cells. In an environment in which those planning attacks might “look like ordinary people going about their everyday business”⁴⁰ analysts may never identify the existence of such groups from collected information. Therefore, there is a need for concepts of decision-making about threats in the absence of specific information or knowledge of threats particularly in circumstances where lives can be lost.

Given the imperfect nature of collected information, which at times appears to be narrowly defined as classified information⁴¹, the sole reliance on such information for issuing threat assessments appears questionable. This is particularly evident when the same information that assessments are made on was described as; fragmented, uncorroborated, lacking in detail and contradictory⁴². Instead, a re-evaluation of what information is available upon which judgements can be made is worth considering, as is evident in two approaches that emerged from the Inquiry. Thus, whilst continuing attempts to identify specific information which could prevent attacks, identifying ‘what can be known’ appears a logical approach.

Conditions for the existence or emergence of threats

The analytical focus on already identified threats was acknowledged during the Inquiry. One analyst testified that “the fascination or preoccupation with Laskar Jihad [a well-documented terrorist group] 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.”⁴³. Concerns over terrorism in South East Asia and the known existence of groups, such as Laskar Jihad, could provide a possible indication that other threats exist. A focus on the broader security environment moves analysis beyond identified actors to consider whether other threats are likely to exist or emerge. Research would be required to identify factors that would indicate the likely emergence of other threats. Nevertheless, it is evident from testimony that a number of factors had been identified that would make threats,

³⁸ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.105

³⁹ Official Committee Hansard, *Security threats to Australians in South-East Asia*, Friday, 28 May 2004, p.452

⁴⁰ Mr Bonighton, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.353

⁴¹ One ONA analyst’s testimony that the Agencies’ “reporting on terrorism in the region was based on the intelligence available to us”. Mr Jones, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 24 September 2003, p.120

⁴² Mr Lewincamp, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 20 June 2003, p.55-56

⁴³ Mr Gordon, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 23 June 2004, p.522

if they did exist, difficult to identify. For example, DIO assessed that “[w]eapons and explosives expertise is freely available in the region, and high-interest individuals can be difficult to track within high volumes of illegal people movements.”⁴⁴ This assessment identifies a number of factors that might encourage the potential emergence of threats or hinder in identifying currently existing threats. Further, increased anti-western sentiment within Indonesia had also been identified as a likely result of the global war on terror⁴⁵.

Another potential factor that emerged during the Inquiry is the permissiveness of the environment, based on the attitudes and actions of authorities in dealing with threats. The contrast between Singaporean authorities (who informed regional nations of the existence and threat from JI) and Indonesia authorities (who were reluctant to believe JI was a threat or act against extremists⁴⁶) is a telling example. The Committee’s final report concluded that, once Australian intelligence agencies were aware of JI, “[i]f there was any notable omission thereafter that contributed to the disaster it was 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”⁴⁷. Such knowledge of the broader environment could be developed prior to identifying specific threats and can potentially be achieved based on information that is available.

Defining national interests

As the national threat assessment agency, ASIO is responsible for assessing threats against Australian interests within the nation and overseas. During the Inquiry ASIO specifically defined Australian interests overseas as encompassing Australian dignitaries, official representatives, commercial business interests and the Australian travelling public⁴⁸. The increasingly global presence of Australians should, therefore, be an important factor in assessing threats and one which information is available. As evident from the Bali bombings, JI did not have to travel to Australia to kill large numbers of Australian citizens. As a result, knowing when and where citizens travel and live when they are overseas appears to be important.

However, despite the large numbers of Australians specifically within Bali, intelligence agencies did not appear to factor this into threat assessments. It was this point that the Committee’s final report took exception, arguing 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 terrorist

⁴⁴ Defence Intelligence Organisation (Department of Defence), *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.13

⁴⁶ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.27

⁴⁷ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.xv

⁴⁸ Dennis Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.5

networks to attack ‘soft targets’⁴⁹. In the six months prior to the attacks, over 20,000 Australians visited Bali every month, compared with 5,000 Australians registered as living in Jakarta (Indonesia’s capital city) during a similar period⁵⁰. Around 239,000 Australians visited Bali in 2001 and over 183,000 in 2002⁵¹. When asked whether ASIO would pay particular attention to the security circumstances in Bali because of the presence of large numbers of Australians, one official 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.⁵²

Of course, tracking individuals in a region of high volumes of legal and illegal people movements is extremely challenging and, in the case of Bali, proved unachievable. A further argument against singling Bali out for assessments was that there were a whole range of Western interests across South-East Asia which could have been targeted, including in Thailand, Malaysia and other parts of Indonesia⁵³. A counter to this is there are numerous areas within South-East Asia where few, if any, Australian citizens travel or live (particularly in large numbers). Australian citizens cannot be killed or injured in large numbers if there are no large numbers of Australians in the location. If analysts assess threats *against* national interests, then defining where citizens are located appears to be a fundamental aspect in arriving at sound judgements about threats. It also provides a potential approach to assist in prioritising limited analytical resources.

Given the acknowledged absence of specific information on attacks, having a general awareness of the location of citizens globally appears both sound and achievable. Knowing where citizens are, coupled with an understanding of the conditions for the emergence of threat and the permissiveness of the environment appears a sound approach in making judgements about threat. Such an approach is not simply shifting from assessments of threat to risk, but focuses the finite resources of intelligence agencies onto the actual purpose of threat assessments, protection of national interests, in the case of terrorism protecting citizens. Using generic information about where

⁴⁹ See Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, Chapter 4

⁵⁰ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.108-109

⁵¹ Foreign Affairs, Defence and Trade References Committee, *Bali 2002: Security threats to Australians in Southeast Asia*, August 2004, p.109

⁵² The Director General agreed with the Chair’s summation that “you are tracking the bad guys—where they are and where they might pop up. You are not so much looking at where the Australians are and what is happening to them.” Official Committee Hansard, *Security threats to Australians in South-East Asia*, 19 June 2003, p.12.

⁵³ Mr Richardson, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 May 2004, p.460. A similar assessment had been made by DIO, which argued that “[w]e had made the assessment that the attack could occur anywhere in Indonesia and therefore no place should be specifically isolated.” Mr Lewincamp, Official Committee Hansard, *Security threats to Australians in South-East Asia*, 28 November 2003, p.348

and when Australian citizens travel overseas assists in developing a context for what the threat is against. Defining national interest in terms of when and where citizens travel overseas is not an attempt to predict attacks. Instead, generic knowledge of citizens' locations provides an initial step for prioritising collection and analysis efforts and establishing a reference for actively looking for the potential emergence of threats or focus efforts on detecting currently unidentified threats⁵⁴.

Conclusion

Analysts' assessments about threats represent the essential part of decision-making in intelligence analysis. This process is of fundamental importance as the results directly influence the decisions made by Government. Unfortunately, in dealing with non-state actors, intelligence agencies and analysts are unlikely to have all the information necessary to make sound or insightful decisions about threat. The small number of people required to carry out mass-casualty attacks, and the difficulty in identifying these groups, means that intelligence agencies might not collect *any* information indicating that an attack is being planned, as was the case with Bali. This requires that intelligence agencies consider alternative concepts for making decisions about threat.

The two approaches considered in this paper recognise the oft quoted observation that intelligence agencies will not necessarily collect specific information on actual attacks. Whilst attempting to collect such information remains a priority, the approaches that emerged during the Inquiry draw attention to information which is available to assist in making judgements on threat. The first approach is the importance of general information to enable judgements on whether conditions exist for the emergence of threats, or existence of yet unidentified threats. Such an approach moves beyond focussing on already identified threats, and recognises that collected information does not necessarily identify all (or even the most dangerous) threats. This is particularly important given the small numbers of people required to undertake major attacks. The second approach is the importance of defining national interests to focus analytical efforts. In the context of terrorism, information on where citizens travel and reside when overseas provides agencies with a method of prioritising collection and analysis in assessing threats as well as a reference point for actively looking for the potential emergence of unidentified threats. As the Inquiry concluded, it is not enough simply to argue that there was no specific information prior to the attacks. If analysts re-evaluate what information is available to better focus analytic efforts towards protecting national interests then there is the potential to make better decisions about threat.

⁵⁴ In the case of large numbers Australian citizens travelling to (and living in) countries like the United Kingdom and United States this is where an analysis of the permissiveness of the environment proves valuable. Given that these nations share similar perceptions of threat and have information-sharing arrangements with Australia, Australian intelligence agencies are able to focus efforts on assessing threats in more permissive threat environments.