Re-shaping Australian Intelligence

Sandy Gordon

Non-conventional security challenges and the information and communications technology (ICT) revolution have radically altered the environment in which Australian intelligence operates. Despite some changes at the margin, Australia's intelligence community is still primarily configured to meet the kinds of challenges it dealt with in the Cold War. This paper argues that the current intelligence architecture is inadequate to deal with Australia's rapidly changing environment. It then suggests how intelligence structures might be re-furbished to provide Australia with a more responsive intelligence performance.

> *That world [post 2010] will require intelligence to be disbursed, not concentrated; open to a variety of sources, not limited to secrets; sharing its information and analyses with a variety of would-be partners, including foreigners and people outside government . . .* Gregory Treverton[1]

Introduction

Those responsible for intelligence[2] in Australia are required to deal with change on two fronts. First, the concept of a tightly contained Australian intelligence community (AIC)[3], as it was constructed during the Second World War and Cold War, is increasingly challenged by the need to accommodate non-conventional security concerns such as terrorism, transnational crime and environmental crisis. Secondly, rapid development in information and communications technology (ICT) poses a significant challenge to the structures and methods of intelligence agencies on the one hand and the relationships between those agencies and their clients in policy and operations on the other.

The rapidly changing intelligence environment was brought into sharp focus by the attacks of September 11, 2001 (henceforth September 11th) and the intelligence failures associated with the 2003 Gulf war. In relation to those events, the US and UK conducted a series of searching inquiries into their intelligence agencies. These inquiries contributed to significant changes to

[1] G Treverton, *Reshaping National Intelligence for an Age of Information*, Cambridge University Press [with Rand Corporation], Cambridge, 2003, p. 20.

[2] The term 'intelligence' can be used in three ways. It can refer to the agencies involved in the production of intelligence, the product of those agencies (whether in written, electronic or oral forms) or the processes that result in this product, such as collection and analysis of information. In this paper the term is used in all three ways.

[3] The term Australian Intelligence Community is more fully explored below. For present purposes it is taken to mean the Office of National Assessments, the Australian Secret Intelligence Service, the Australian security Intelligence Service and the various services under the auspices of the Department of Defence.

intelligence agencies and architecture, especially in the US.[4] In Australia, there has been only one major inquiry since the first Hope Royal Commission, which reported in 1977. This was by retired senior bureaucrat Phillip Flood in 2004.[5]

According to his terms of reference, Mr Flood was directed to report on the foreign intelligence community. He could also consider that community's relations with the domestic security agency, the Australian Security Intelligence Organisation (ASIO), but chose not to do so. No reference was made to other domestic or foreign intelligence capabilities, such as those embedded in executive agencies of first response such as the Australian Federal Police (AFP), the Australian Crime Commission (ACC), the Australian Customs Service (Customs), Coastwatch, the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA) and the Department of Transport and Regional Services (DOTARS).[6] Partly because of these limited terms of reference, the Flood Report brought down an essentially *status quo* finding that 'The architecture designed by Justice Hope in the 1970s for the Australian intelligence community remains valid, and there is no need for fundamental structural change'.[7]

There have, however, been some changes outside the ambit of the Flood Report. These were mostly introduced to deal with the challenges posed by the events of September 11th. Although some of these have been quite significant, they do not change the basic architecture that provides for a high degree of separation between the AIC and the executive agencies of first response. These latter agencies are the ones that are most heavily engaged in dealing with the challenges of non-conventional security threats.

This paper discusses non-conventional security and the ICT revolution as they impact on Australian intelligence, with reference to the evolving post-September 11th US model for the sake of comparison. It assesses whether the totality of change imposed on Australian intelligence since September

[4] In the US, the most prominent of these are 'The 9/11 Commission Report' (*Final Report of the National Commission on Terrorist Attacks upon the United States*), 'The FBI Inquiry' (Department of Justice, *A Review of the FBI's handling of Intelligence Related to the September 11 Attacks*) and the *Report on the US Intelligence Community's Prewar intelligence Assessment on Iraq* (Senate Select Committee on Intelligence). In the UK the major report was the 'Butler Report' (*Review of Intelligence on Weapons of Mass Destruction*). A more limited report into the death of Dr Kelly was conducted by the Rt. Hon. Lord Hutton (Hutton Inquiry) titled 'Investigation into circumstances surrounding the death of Dr David Kelly' (http://www.the-hutton-inquiry.org.uk).

[5] Australian Government, *Report of the Inquiry into Australian Intelligence Agencies* ('Flood Report'), July 2004, Commonwealth of Australia, Canberra, 2004, http://www.pmc.gov.au/publications/intelligence_inquiry. All references to the Flood Report are drawn from this source, including page references. A second Hope Inquiry was conducted in 1983, but was far more narrowly based.

[6] See Flood, *Ibid*, p. 1. One quarter of DOTARS staff is now involved with transport security.

[7] Flood, *Ibid*, p. 83.

11th has been adequate to deal with the radically altered environment. It then outlines a new approach to intelligence architecture in Australia that could provide a better capability to meet these challenges.

The Australian Intelligence Community and the Canberra Bureaucratic Framework

According to the definition used in this paper, the AIC is made up of a tight, Canberra-based network of relatively small government agencies. It consists of the Office of National Assessments (ONA) at the apex; the Defence Intelligence Organisation (DIO) and other Defence intelligence agencies such as Defence Signals Directorate (DSD) and Defence Imagery and Geospatial Organisation (DIGO); Australia's overseas spy agency, the Australian Secret Intelligence Service (ASIS); and ASIO.

Some would not accept that ASIO should be included as a fully-fledged member of the AIC. ASIO operates primarily in the domestic sphere and is governed by specific legislation that gives it a distinct role in relation to domestic security intelligence somewhat similar to ONA's role in foreign intelligence.[8] Although such a view is valid in strictly legal terms, we argue in this paper that ASIO is part of a collective that can validly be covered by the label 'AIC'. We note a strong similarity in that both 'sides' relate closely to a small body of departments that contribute to the development of policy at the elite level in Canberra. They thus collectively have a distinct identity that separates them from intelligence areas in the executive agencies of first response. Intelligence units in the latter are regarded primarily as contributing to the operations of their home agencies rather than to the development of policy at the highest level of government. It is precisely this 'cut-off' between 'policy' and 'operations' that is of particular concern in Australia's rapidly changing security environment (see below).

Another factor in the tightly bound nature of the AIC (including ASIO) relates to the genesis of modern intelligence in Australia. Much of Australia's foreign intelligence is derivative, especially from the US and UK. This situation grew out of the Second World War and Cold War, periods during which Australia and other Anglophone allies (known as 'the cousins')[9] were dependent for intelligence, especially signals intelligence (SIGINT), on the far greater spending and capability of the US and UK. In the context of the emergence of the Cold War, it was an unwritten condition of the continuation of this access that intelligence provided for Australian and other non-US-UK

[8] The Director General of Security (who is also head of ASIO) has a legislated role to coordinate and report on domestic security intelligence similar to the role of the DG of ONA in relation to foreign intelligence.

[9] The 'cousins' originally consisted of the US, UK, Canada, Australia and New Zealand. Although some intelligence is still shared with New Zealand, following Wellington's refusal to allow US nuclear vessels to pass through NZ waters it is no longer a fully-fledged member of the 'cousins'.

cousins should be tightly held lest key secrets fall into the hands of Soviet agents.[10] This need to protect highly sensitive intelligence in the Cold War setting was also the reason that ASIO was the first major post-war intelligence agency to be established, with the direct assistance of the British domestic security intelligence agency, Military Intelligence 5 (MI5). It is another reason that ASIO has in practice come to be seen as integral to the AIC.

Eventually, as confidence grew, intelligence was more readily shared amongst the cousins. As far as Australia was concerned, however, the intelligence exchanges involved in this sharing process drew from a small, inner circle that could be known to, and trusted by, Australia's powerful intelligence allies. The AIC in its present form thus grew out of and developed its mores from the Cold War – a condition that significantly shapes it even a decade and a half after the fall of the Berlin Wall.

Very closely aligned with the AIC agencies are the committees and departments that tightly control the intelligence apparatus. This control cascades down from the National Security Committee of Cabinet (NSC)[11], through to the Secretary's Committee on National Security (SCONS) and on to the various departments that are responsible for determining intelligence directions and collection priorities at lower levels. Concerned departments include the Department of Defence (the 'parent' department of DIO, DSD and DIGO), the Department of Prime Minister and Cabinet (PM&C, the parent department of ONA), the Department of Foreign Affairs and Trade (DFAT, which 'hosts' ASIS) and the Attorney-General's Department (AG's, which has policy responsibility for ASIO).

A second reason for the tightness of the AIC relates to the nature of bureaucratic hierarchies in Canberra. At the apex of the bureaucratic pyramid is a group of 'policy' departments consisting of Treasury, DFAT and PM&C. DFAT is an elite department that controls its own recruiting according to very high standards of entry. PM&C, on the other hand, draws expertise from other specialist departments in order to 'second-guess' and to an extent control them. Its power derives from its role as principal bureaucratic advisor to the Prime Minister and its coordination role for the federal bureaucracy as a whole. In the area of international relations and security it happens to draw heavily from DFAT – thus forming a natural alliance between the two in this

[10] P Murphy, 'Exporting a British Intelligence Culture: The British intelligence community and decolonisation, 1945-1960', p. 2, www.psa.ac.uk/cps/2004/Murphy.pdf.

[11] The NSC consists of the PM, Treasurer, Minister of Defence, Minister of Foreign Affairs and Attorney-General. Other ministers are seconded to the NSC when specific issues relevant to their portfolios are being addressed. Senior officials also attend the meetings: the secretaries of the departments of the Prime Minister and Cabinet, Defence and Foreign Affairs and Trade; the Chief of the Defence Force; and the directors-general of the Australian Security Intelligence Organisation and the Office of National Assessments. Other secretaries and the Commissioner of the Australian Federal Police may be called upon to attend when needed.

area. As internal security has become more important to overall security concerns (see below), the Attorney-General's Department has also grown in profile in terms of the AIC's controlling bureaucratic framework. Defence has a natural place in the controlling hierarchy by virtue of its control over significant security and intelligence assets.

The tightness of control amongst this group is to an extent increased by the fact that there is considerable interchange between the personnel of the elite departments. DFAT is especially benefited in the exchange arrangements that have evolved. For example, since its foundation, every head of ONA has been a DFAT officer. Many of the heads have returned to DFAT to higher positions. The First Assistant Secretary in charge of the International Division of PM&C is a seconded DFAT officer who would in normal circumstances be expected to return to DFAT. Currently, the heads of ASIS and ASIO are also former DFAT officers. This is not to argue that DFAT officers are not highly talented or that they should be excluded from such positions, but rather to make the point that the crafts of intelligence and diplomacy are very different in their essence, involving differing skills sets and attitudes to the construction of policy. Given these differences, such positions should be rather more open – for example to career intelligence officers – than in fact appears to be the case.

During the Cold War and its aftermath, these bureaucratic structures left little if any 'room at the table' within the AIC for operational agencies and departments of first response. Although this situation was little noticed in the Cold War when threat was perceived to be overwhelmingly of a military nature, it did appear to some increasingly anomalous in the post-Cold War environment, when threat was increasingly perceived to be non-conventional in character, involving threats such as transnational crime, terrorism, HIV/AIDS, various quarantine issues and environmental security.[12] It is to a discussion of these non-traditional challenges that we now turn.

The AIC and Non-Traditional Security Challenges

During the years following the end of the Cold War, the AIC was heavily oriented to 'foreign intelligence' as a result of its Cold War experience. The exception to this was ASIO, which had a remit to cover domestic security and which had focused substantially on terrorism since the Hilton bombing of 1978.

After the end of the Cold War, the rapid onset of globalisation and lifting of power bloc strictures acted as drivers of the new non-conventional threats

[12] For a fuller discussion of this shift in Australia's Asian region see A Dupont, *East Asia Imperilled: Transnational Challenges to Security*, Cambridge University Press, Cambridge, 2001.

that challenged Australia's security apparatus. Many of the new non-conventional challenges were, however, dependent both on a 'push' (or supply) factor from weak or failing states in the developing world and a 'pull' (or demand) factor from developed countries such as Australia. It is therefore correct to think of the advent of such challenges more as a 'seamless web' than as a situation forced on developed countries from the external world.[13] This development thus amounted to a folding together of the realms of domestic and foreign security intelligence.

The domestic-foreign linkage operates at its most intense for non-conventional security threats like terrorism and transnational crime. For example, the international heroin trade – driven by bourgeoning supply in failing states like Burma and Afghanistan – resulted in the deaths of over 5000, mostly young, Australians in the 1990s. But Australian research also shows that certain structural problems *within* Australian society have been powerful contributing factors to drug abuse of the kind that has negative outcomes such as heroin-related morbidity and mortality.[14] Similarly in the case of terrorism, if one examines the so-called 'home grown' terrorism attacks on the London underground of July 2005, one can see a clear nexus between global events centring on South/South West Asia and the Middle East and the situation of Muslims in the UK itself.[15]

This domestic-foreign nexus, which is often intrinsic to the nature of non-conventional security threats, poses a particular challenge to security systems, such as the one in Australia, in which there are powerful structural factors effectively separating foreign and domestic intelligence.

It would be wrong, however, to think of this growing relationship between domestic and international threats as being confined wholly to non-conventional security concerns. Even traditional state-on-state security is frequently critically affected by non-conventional security. For example, the Timor crisis (which had some elements of a traditional state-on-state situation) and 'boat people' emergency (a non-conventional security situation) happened to occur simultaneously. The boat people crisis also had critical domestic elements as well as powerful foreign drivers. The two crises came to leverage off each other in terms of their overall impact on Australian security.[16]

[13] For a description of the combined role of globalisation and failed or failing states in this process see J-G Gros, 'Trouble in Paradise', *British Journal of Criminology*, vol. 43, no. 1, Winter 2003, pp. 63-80.

[14] See for example C Spooner and K Hetherington, 'Social Determinants of Drug Use', National Drug and Alcohol Research Centre, University of NSW, Technical Report No. 228, NDARC, Sydney, 2005, p. iv and *passim*.

[15] Some of the alleged bombers had received training in Pakistan. As British Muslims, they clearly had deep-seated problems with their status and situation in the UK.

[16] The Timor crisis and consequent serious deterioration of Australia's relationship with Indonesia left Australia highly exposed to Indonesia using the backlog of asylum seekers in

By the time non-conventional threat reached its 'tipping point' in the Australian psyche on September 11th, Australia had done somewhat less to change the character of its intelligence community to deal with the new circumstances than had the US and UK. During the Cold War and its immediate aftermath, the US and UK intelligence structures were broadly similar to those in Australia in terms of the existence of a tightly controlled, defence-oriented, intelligence community largely divorced from those agencies dealing with non-conventional threats. However, there were differences in nuance. In both the US and UK, circumstances forced the intelligence agencies at least in part to break out of their traditional defence intelligence shackles earlier than Australia.

Partly in a search for relevance in the aftermath of the Cold War and partly at the behest of President Clinton, in the US the CIA and Defence-related agencies used the post-Cold War environment in order to focus on non-traditional issues, especially transnational crime and the 'war on drugs'. In addition, it was apparent at least since the first bombing of the World Trade Center in 1993, that the US had a serious terrorism problem. This focus on terrorism was reinforced by the Khobar Towers bombing of 1996, the East African embassy bombings of 1998 and the attack on the USS Cole in 2000. Although the intelligence failures prior to September 11th, as set out in the *9/11 Commission Report*, illustrate that the reform process was inadequate, there was a heavier focus on some elements of non-traditional security in the US than in Australia.

Due to the long-standing security problem in Northern Ireland, UK intelligence also had to confront non-traditional threats earlier than Australia. As a result of this problem, the UK agencies had a stronger focus on internal security. They also developed a close working relationship with law enforcement, especially Special Branch of the Metropolitan Police. The military was itself involved in helping to stabilize the situation in Northern Ireland, so its agencies, such as the Defence Intelligence Staff (DIS) and the unit-level tactical intelligence groups, were also heavily involved in this 'non-traditional' work. That situation flowed through naturally to the post-September 11th period.

That is not to say that Australia had not undertaken at least some changes prior to September 11th with a view better to integrate operational intelligence provided by executive agencies and strategic intelligence of the kind provided by the AIC. As far back as the 1980s, ASIO and DIMIA had started to cooperate closely on identifying arrivals deemed to constitute a security risk.[17] ASIO and the AFP had also established mechanisms for closer

Indonesia as a means to pressure the Australian government, either by refusing to cooperate, or worse, actually facilitating their passage to Australia.

[17] Interview with a recently retired ASIO officer.

cooperation at all levels of the organizations, including regular meetings of senior officers. But these attempts achieved only limited success and by the end of the 1990s (at least from the perspective of the AFP) there were still significant anomalies and oversights in the system.[18]

By 1999, concern about the arrival of 'boat people' was starting to drive a more significant period of change within the AIC. Max Moore-Wilton, the powerful Secretary of PM&C and politically close to the government, 'bashed bureaucratic heads together' in the AIC to force the change in response to a number of attempts by mainland Chinese to enter Australia by boat in that year.[19] Realizing the political fallout that could be caused by a continuation of such arrivals, Moore-Wilton forced ONA to take on the role of coordinating the gathering of intelligence on illegal migration. With the arrival of increasing numbers of South West Asians via Indonesia, ONA's coordination role was quickly extended to embrace DFAT, the AFP, DIMIA, Customs, Coastwatch and the relevant Defence agencies. New resources were provided and new laws passed increasing the penalties for people smuggling.[20] This was the first time that ONA had taken transnational crime seriously as a security concern.[21]

The requirement to stage a trouble-free Olympic games in Sydney in 2000 also changed the balance within the AIC. Terrorism and other non-conventional concerns, rather than state-on-state security threats, were centre-stage in terms of Olympic security. Under the Olympic security architecture, ASIO was placed in a coordinating position *vis à vis* the international intelligence community and Commonwealth government. Its position within the AIC was enhanced by its role in the Olympics, a situation that has continued in the post-September 11th climate. This enhanced role in turn reflected on the position of the Attorney-General's Department in the national security framework. The Attorney-General's portfolio responsibilities covered domestic security, law enforcement, Customs and Coastwatch, which in turn captured much of the non-conventional security agenda rapidly coming to the fore.

Despite the lessons of the 'boat people' crisis, the requirements to stage the Olympics and the lessons of September 11th, as late as February 2002 ONA still had no specific branch to deal with transnational issues. At that stage, such issues were handled within the strategic analysis branch – which itself had earlier on been abolished and then re-established.[22] (But to be fair, ONA

[18] Interview with senior, recently retired AFP officers and experience of the author.
[19] See D Marr and M Wilkinson, *Dark Victory*, Allen and Unwin, Sydney, 2003, p. 39.
[20] *Ibid*, pp. 39-40.
[21] Marr and Wilkinson reported that ONA had not really taken people smuggling seriously as a security issue. *Ibid*, p. 39.
[22] Evidence of K Jones, Director-General of ONA, to Senate Finance and Public Affairs (Estimates) *Legislative* Committee, Monday, 18 February 2002, Commonwealth of Australia, Canberra, Hansard, 2002, p. 136.

was then a very small organization, with only between about 30-40 analysts at any one time). This reluctance, while somewhat excusable in terms of resourcing issues within ONA, is indicative of a wider failure of the AIC in the 1990s to recognize the changing strategic environment and cater for it.

The consequences of this failure in terms of the performance of the AIC are illustrated by three intelligence lapses relating to Australia's near region, a region in which Australia's intelligence reach should have been highly effective. These examples do not include perceived failures that have received more prominence in the public discourse, such as Iraq or East Timor. Troubling as these might be, they do not involve the type of failures that are most telling as illustrations of the AIC's reluctance to incorporate whole-of-government intelligence, as it should have done in response to the rising level of non-conventional threat.[23] It is this type of failure with which we are most concerned in this paper.

The Sandline crisis of 1997 involved the hiring by the Chan government in PNG of a mercenary firm called 'Sandline' (an offshoot of the South African firm, Executive Outcomes). The purpose of the venture was to train PNG's Special Forces and use them and Sandline mercenaries to capture or kill the leadership of the Bougainville revolt and re-open the Panguna copper mine. Sandline was to be paid US $36 million and several ministers of the PNG government were also allegedly paid off by Sandline. Parts of the story were originally broken by a journalist with *The Australian*, Mary Louise O'Callaghan.[24] The ABC's then correspondent in Port Moresby, Sean Dorney, wrote a book on Sandline (*The Sandline Affair*) in which he characterises the Australian intelligence lapses in the following terms:

> …despite the huge number of [Australian intelligence and military] personnel engaged in doing nothing else but keeping the Australian Government informed about what goes on in PNG (and despite the sophistication of Australia's eavesdropping capabilities) there were still significant pieces of information missing [at the time of Foreign Minister Downer's visit to Port Moresby on 19 February, 1997].[25]

[23] In the case of Iraq, Australia was almost wholly dependent upon foreign intelligence, especially from the US and UK, since Iraq was well outside Australia's intelligence purview. Andrew Wilkie's arguments about failed interpretation of that intelligence and political bias may well be sound, but our overriding concern here is about the capacity of intelligence to feed from the operational base, and in that sense Wilkie's argument is not strictly relevant. See A Wilkie, *Axis of Deceit: The story of the intelligence officer who risked all to tell the truth about WMD and Iraq*, Black Inc., Melbourne, 2004). In the case of East Timor, it is the author's view that the government knew what was likely to occur, but had no policy option but to act as it did in the circumstances, the views of Lt. Colonel Lance Collins notwithstanding. Clearly, however, Collins acted in good conscience and good faith.

[24] It is possible that Ms O'Callaghan was briefed by government elements in order to alert PNG to the fact that Australia was aware of the situation.

[25] S Dorney, *The Sandline Affair: Politics and Mercenaries and the Bougainville Crisis*, ABC Books, Sydney, 1998, p. 222.

According to Dorney, the Australian officials who comprised the AIC were also completely unaware of the plan of the Commander of the PNG Defence Force, Brigadier-General Gerry Singiroc, to oust the mercenaries in Operation *Rausim Kwik*.[26] This plan by Singiroc directly opposed the PNG government and in effect amounted to a 'mini coup'. The planned Singiroc 'coup' was actually discovered not by the AIC but the AFP liaison officer in Port Moresby, who was able to warn the Royal Papua New Guinea Constabulary (RPNGC) and the Australian government prior to the event. This warning enabled the RPNGC subsequently to play a key role in ensuring that the matter did not slip out of hand into a fully-fledged coup.[27] Dorney is also damning of the intelligence provided within the ONA document (classified AUSTEO) that was leaked prior to the Pacific Forum meeting. He refers to the document as an 'extraordinary misreading of [Deputy PM Chris] Haiveta …The document was wrong about all three of its predictions in relation to Haiveta'. Dorney finally comments 'It was the tone of superiority [of the leaked AUSTEO document], as much as the misinterpretations, that did the damage'.[28]

Ironically, even though the AFP had supplied the evidence of the forthcoming Singiroc 'coup', and even though it had people security cleared to the highest level, it was denied access to subsequent cables from the Australian High Commission in Port Moresby on the grounds that the information was too sensitive.[29] This bizarre outcome illustrates not only the isolation of the AIC in an area that should have been its heartland of operations, but also the at times absurdity of its information dissemination policies. The two were, of course, connected.

The next intelligence problem to confront Australia that was initially beyond the interest and intelligence reach of the AIC was the so-called 'boat people' problem mentioned briefly above. The influx of boat people through Indonesia had been evident to many people outside the AIC for many years prior to the intervention by Moore-Wilton in 1999. Indeed, DIMIA (then DIEA) was well aware of the problem when interviewed by the author in 1995. At that stage, many people smuggling trips were entrepreneured by a Pakistani facilitator based in Cupang, West Timor.[30] By 1998 it was a standing joke amongst those who knew in DIMIA and the AFP that Indonesian captains and crew members used to relish a few months in Darwin jail, where they could get their teeth fixed and earn a few dollars a day to take back to Indonesia. However, this operational knowledge had not yet been

[26] Dorney, *Ibid*, p. 261.
[27] Interview, AFP officer, August 2005, and knowledge of the author of these events.
[28] Dorney, *op cit*, p. 338.
[29] Knowledge of the author. A number of senior and intelligence staff in the AFP were at the time cleared to a level well above the classification of this particular document.
[30] Author's interview with a senior DIEA official, 1995.

'actualised' as a political issue, and hence was virtually un-pursued by the AIC in terms of its work and interests.[31]

But the starkest illustration of the isolation of the AIC foreign intelligence community from the operational base is provided by the so-called 'children overboard' affair. In this incident involving suspected illegal entry vessel (SIEV) 4, it was initially reported by the Navy that in the early hours of 7 October 2001, asylum seekers had thrown children overboard in an attempt to prevent their vessel being forced away from Australian waters. This information was retailed rapidly to government and subsequently used a month later in the run-up to the national election of November 2001.[32] Photos of children who had allegedly been thrown over-board being rescued by Australian sailors were provided to the media. The fact that they were actually photos of children being rescued from the sinking vessel the next day was never clarified to the Australian people prior to the election.

Even though members at all levels within the Navy were well aware as early as *10 October* that no children had been thrown overboard, ONA reported to the Prime Minister's office on 7 November that children had, indeed, been thrown overboard. This report was referred to by the PM in a public statement on the 7 November. Despite a partial retraction by ONA on the 8th , in which the agency explained that it had probably based the previous day's report on press reporting and ministerial statements at the time of the original incident or shortly thereafter, but that it was unsure whether Defence reporting was also involved, the PM again referred to the ONA report publicly on the Friday 8th.[33] A definitive correction was not made until after the election that weekend. When questioned about this in the Senate Estimates Committee, the ONA Director General said that ONA was still unsure before the weekend whether or not children had actually been thrown overboard and was unclear whether its original report had relied solely on ministerial and press statements, or whether there was also an element of defence reporting.[34]

There are two important features of this event from an intelligence point of view. First, despite the span of a month from the time of the original incident, ONA evidently depended on press and ministerial reporting rather

[31] Knowledge of the author.
[32] For background on the SEIV 4 incident see Parliament of Australia (Senate) 'Select Committee for an inquiry into a certain maritime incident' tabled on 23 October 2002, http://www.aph.gov.au/senate/committee/maritime_incident_ctte/; and Marr and Wilkinson, *op cit*.
[33] See M Kingston, 'What servants are for' *Sydney Morning Herald*, 27 June 2002 http://www.smh.com.au/articles/2002/06/27/1023864633818.html; A certain maritime incident caps. 3 and 4.
[34] For Mr Jones' evidence to the senate Estimates Committee, see Evidence of Kim Jones, Director-General of ONA, to Senate Finance and Public Affairs (Estimates) *Legislative* Committee, Monday, 18 February 2002, Commonwealth of Australia, Canberra, Hansard, 2002, pp. 135-43.

than a more robust line of contact with the operational arm of government involved, in this case the Navy, or the Navy through DIO. This led to a situation in which the Director-General, and evidently those immediately around him, were ignorant of what was common knowledge throughout the Navy and, indeed, in senior echelons of the relevant areas of the public service. A true operational feed would have involved a much closer nexus between the operation and the DIO, and through DIO, ONA. A second implication is that ONA was at the time apparently short of resources in the transnational area. Certainly, this is about the only possible explanation of the failure of the organisation to have more robust intelligence on hand. Curiously, this telling example of the failure of Australia's premier intelligence organisation is not discussed in the Flood report.

The third example of the failure of the government to incorporate and assimilate important information and advice from its operational agencies is provided by the crisis in the Solomon Islands. On 30 June, 2000, the government of Bartholomew Ulufa'alu was overthrown in a coup. This coup in part resulted from the actions of the Solomon Islands (SI) armed police. The SI Police was dominated by people from the island of Malaita, a group that was in turn being threatened on the island of Guadalcanal, the location of the capital, Honiara, because of their dominant position in the bureaucracy and rapid acquisition of land on Guadalcanal.[35]

Prior to the coup, the AFP had a two person contingent attached to the SI Police. The AFP contingent advised the AFP of the rapidly deteriorating situation within the SI police. The AFP recommended that Australia should provide further support to stabilise the SI police, including by placing an Australian in the position of Commissioner and providing more Australian police 'on the ground'. At the same time, PM Ulufa'alu also made a similar request for 50 extra police. In conveying the request he evidently pointed out that, at that time, numbers of armed militants were small and the vast bulk of the population did not support them. He also said that the leader of the opposition would support outside police assistance.[36] The request for intervention was also strongly supported by New Zealand.

The AFP support for the SI Government's request was, however, opposed within an inter-departmental committee (IDC) by DFAT on the grounds that

[35] For an account, see T T Kabutaulaka, 'A Weak State and the Solomon Islands Peace Process', East West Center Pacific Islands' Development Series, No. 14, April 2002, especially page six for the role of the police.

[36] Some of these details are drawn from an article by Duncan Kerr, Deputy Leader of a parliamentary delegation to the SI some weeks before the coup. They describe the meeting between the delegation and the PM. While Kerr is a Labor politician, the fact that he was part of a parliamentary delegation would indicate the basic facts of the article are accurate. See 'The shocking reality of Downer's dirty little Solomon Islands' secret', ON LINE opinion, posted 28 July 2003, http://www.onlineopinion.com.au/view.asp?article=577.

the situation in SI was still unclear.[37] (As late as January 2003, Foreign Minister Downer said 'Sending in Australian troops to occupy Solomon Islands would be folly in the extreme'.)[38] In answer to a parliamentary question, the Prime Minister explained that the government was reluctant to commit unarmed police into a dangerous situation in the SI.[39]

Shortly after the Ulufa'alu government's request was turned down by Australia, it fell in a coup that resulted significantly from the decay of the SI police and provision by them of arms to the Malaitan rebels.[40] Later in 2000, as a result of the Cairns Agreement, a force including 50 regional police was inserted, but by that time the situation in SI was on a downward spiral. It took a substantial intervention in the form of Regional Assistance Mission to the Solomon Islands (RAMSI) in 2003 to reverse this situation. Part of the problem was that the successors of the Ulufa'alu government were far less willing or competent to stabilise the situation than was the Ulufa'alu government. It has been estimated that RAMSI will cost as much as $1.3 billion by its conclusion.[41] Although it is impossible to know with any certainty what might have happened had Australia intervened when requested by the SI government in 2000, it is reasonable to suppose that a timely intervention by Australia at the time of the Ulufa'alu government's request may well have been sufficient to stabilise the situation at far less cost to Australia and the SI community.

Although the position of the Australian government in 2000 may have reflected its policy position as much as any intelligence advice, the uncertain nature of the intelligence advice seems to have been an important contributing factor to the decision not to intervene in that year. While the actual wording of AIC reporting in 2000 cannot be conveyed in this paper, the Flood Report notes of it that

> In general, the product [of the ONA and DIO] was more robust in the post-June 2000 period than in the lead-up to the June 2000 coup. Pre-June 2000 reporting was not inaccurate, but generally failed to provide assessments that did much more than monitor events. Neither organisation predicted the coup, although both had recognised the potential for such an action and either dismissed its immediate likelihood or simply highlighted the threat. In the case of DIO, setting aside the specific question of whether the coup should have been predicted, the reporting did not engage operational planners in the practical way that DIO product ideally should.[42]

[37] Knowledge of the author.
[38] Quoted from *The Australian* of 8 January 2003 in an article by Tony Wright, 'High Noon in the Solomons', *The Bulletin*, 9 July 2003.
[39] Department of Foreign Affairs and Trade, Question without Notice, (Question No. 2101), 6 June 2000, http://www.dfat.gov.au/qwon/1999_2001/000606_solomons.html.
[40] Kabutaulaka, *op cit*, p. 6.
[41] ABC Radio 'Correspondents Report', Sunday 10 July 2005.
[42] Flood Report, *op cit*, p. 46.

The three examples of intelligence inadequacies on the part of the AIC cited above all relate to failures to derive a satisfactory process of information exchange with the arms of government charged with dealing with emerging non-conventional security threats at the operational level. Against this position, it might fairly be argued that the situation was transformed by the re-structuring of intelligence following September 11th. We therefore need to ask what changes were actually made following that event.

At the level of broad strategic control over the AIC, the changes have not been profound. The NSC has not been expanded to include representation from relevant agencies. It consists of the PM, Treasurer, Minister of Defence, Minister for Foreign Affairs, Attorney-General and other ministers seconded as necessary. Senior officials who also attend meetings as a matter of course include the secretaries of the departments of the Prime Minister and Cabinet, Defence, and Foreign Affairs and Trade, the Chief of the Defence Force and the directors-general of ASIO and ONA, but not other relevant secretaries or the Commissioner of the AFP (who may be called upon to attend when needed). The Commissioner of the AFP still does not have a permanent place on SCONS.

Under new arrangements introduced in the aftermath of September 11th, a terrorism coordination mechanism, known as the National Counter-Terrorism Committee (NCTC), was established to coordinate policy between states and the Commonwealth. Significantly, the NCTC is chaired by PM&C and a leading state government official rather than a member of the AIC or the Attorney-General's Department. The latter had previously assumed the coordination role through its SAC-PAV committee.[43] The Protective Security Coordination Centre (PSCC), also part of AG's portfolio, has been enlarged and remains the principal coordination mechanism for operational matters. It also coordinates training.

September 11th further provided an incentive for the DOTARS Office of Transport Security (OTS) and ASIO to establish a closer working relationship. This involved ASIO providing the OTS with major transport sector threat assessments and risk management of the potentially most significant terrorist targets. OTS was thus drawn in as a major consumer, and contributor to the intelligence process.[44] At the operational level, ASIO and the AFP formed the Joint Terrorist Tracking Unit (JTTU) with a view to ensuring that both organizations coordinate on the identification and tracking of targets. The newly formed ACC also has a counter-terrorism intelligence role and the Director-General of Security sits on its board.

[43] The NCTC Executive Committee meets regularly, whereas the NCTC itself meets only bi-annually to set broad direction.
[44] Interview with a recently retired ASIO officer.

In terms of the gathering and analysis of intelligence (as distinct from operations and policy), ASIO was also given the role of hosting a 'fusion centre', the National Threat Assessment Centre (NTAC). NTAC consists of ASIO, ASIS, DIO, ONA, DOTARS, DFAT and the AFP. Customs, Coastwatch and the ACC are not directly involved (in some cases by choice) but provide inputs to the NTAC. NTAC provides a '24/7' intelligence and watch house facility and is responsible for recommending travel advisories to DFAT and setting the threat level. Rather than working from a fully-fledged data warehouse facility, our understanding is that it involves participating agencies reaching into their own databases to conduct intelligence analysis and research. The significance of this approach over a data warehouse type arrangement will be discussed below.

Despite these changes, the Australian intelligence agencies continue to exist within a basic framework in which AIC members, especially those agencies involved in foreign intelligence, are largely separated from other aspects of government, including executive agencies and their intelligence units.

In terms of security intelligence, the Director General of Security (also the head of ASIO) continues to be responsible for 'intelligence' while the AFP takes over when matters shift from intelligence to an impending prosecution (that is, anything involving the gathering of 'evidence').[45] This division is in part a reflection of the perceived security need for a highly professionalised intelligence service to catch 'spies' during the Cold War; in part of the dominance of ASIO in domestic security intelligence matters of central concern (such as those relating to the Cold War); and in part due to the concern of Australians not to have police messing around in 'the political underwear drawers' of the nation. This latter concern was reinforced over the years by some spectacular failures of the various police 'special branches', some of which had been used to garner dirt on opposition members and other VIPs.[46]

Such an arrangement gives comfort in terms of the Australian people's well-conceived concern about the police having a political intelligence function.

[45] In law enforcement, intelligence is generally taken to be analysed information pointing to possible guilt whereas evidence is collected and presented according to the laws and rules of evidence in order to establish guilt in court. It is worth noting that in the US, the FBI fulfils both roles. The author's own view is that the two roles could be more closely combined in Australia. Any loss of civil rights or privacy would be more than offset if the trade-off could be a retraction of some of our increasingly draconian counter-terrorism laws. Such an arrangement would be both more effective and fairer.

[46] Once the concern about Communism diminished with the end of the Cold War, the NSW Police Special Branch (for example) was notorious for focusing on the behaviour, including sexual behaviour, of VIPs. A NSW Police Integrity Commission report to Parliament noted that 75% of the Special Branch's work prior to its abolition in 1997 was involved with the monitoring of VIPs. See NSW Police Integrity Commission, *Report to the Parliament Regarding the Former Special Branch of the New South Wales Police Service*, p. 6, http://www.pic.nsw.gov.au/PDF-files/Spec.Brch.pdf.

But it also results in a number of operational problems, especially in terms of allowing for the implementation of intelligence best practice. As discussed in greater detail below, best practice in policing currently involves a near 'seamless web' between policy development, operations and intelligence. The cut-off between ASIO and the AFP, and intelligence and evidence, does not permit the full benefits of the latest technologies and techniques to be realized.

A further problem with the separation of functions between ASIO and the AFP arises in relation to the intelligence-evidence distinction. Some of the information gathered in an intelligence operation is potentially very important as evidence, should a case ever go to court. (Equally, evidence at a crime scene can provide valuable sources of intelligence.) Yet if not actually gathered as evidence (that is, in ways admissible in court) it cannot serve any evidentiary purpose. Moreover, it is very difficult to determine at which point criminality occurs in an intelligence operation if one is not knowledgeable about the legal situations involved. Police, according to their sworn role as constables, carry the discretion and authority as individuals to arrest (seek prosecution) or not arrest. ASIO officers carry no such legal authority. Especially since September 11th, ASIO has attempted to mitigate any negative effects from this separation by gathering its intelligence according to evidentiary requirements.

The AFP-ASIO separation also presents problems in terms of the requirement for police to respond urgently to dangerous situations. They need all the intelligence at their fingertips in order to do so effectively. At the operational level, the AFP has developed its own quasi-intelligence system to enable it to respond quickly to emerging situations.[47] (It is true that the development of the JTTU to an extent mitigates this problem, but only in the case of jointly selected targets.)

The effects of the artificial cut-off between the AIC and operational agencies like police and Customs are accentuated by the legal and funding arrangements that have historically 'belonged' to each side of the equation. Equally, the separation has highlighted the potential resource imbalance in the context of the rising salience of non-conventional security issues.

In terms of a high technology capability to interdict and decrypt communications, Defence has the lion's share of the resources. Defence also maintains the capacity for much of the 'brown' and all of the 'blue' water intervention and higher-level Special Forces action (the rough equivalent of special weapons and tactics – SWAT – in policing).

[47] In this system, which is maintained separately from wider AFP intelligence, the relevant area maintains its own tactical intelligence database acquired from its operational experience.

These attributes are vital to interdicting some forms of transnational crime, in some circumstances. They have been used in this capacity in numerous situations, from the anti-people smuggling campaign waged by the Howard government from 1999 onward, to the raid on the North Korean drug vessel, *Pong Su,* as it attempted to flee Australian waters in 2003. There are also numerous examples of international signals interdiction on behalf of law enforcement, but for obvious reasons they cannot be cited here.

Although considerable capabilities reside with Defence, laws, regulations and protocols protecting the privacy of Australians limit their use in terms of fighting transnational crime and terrorism. Where Australian citizens or residents are involved, permission to use DSD or DIGO material for these purposes must be obtained from the Minister for Defence, and the case must relate to an indictable offence. While the latter may not seem to be a problem, in many cases in intelligence operations no indictable offence is immediately apparent even if one is suspected. Moreover, where DSD-derived information may be involved in the inception of a case, cover is needed to ensure that it is not exposed in any trial that may eventuate.[48]

In addition to problems relating to privacy and information security, the Department of Defence is also unwilling to sacrifice the 'crown jewels' on something it considers important, but not its 'core business'. The 2000 Defence White Paper makes it clear that Defence accepts that 'military operations other than conventional warfare' constitute a rising trend. The document, however, regards defence of Australia from military attack as the most important responsibility of the defence forces.[49] That is not to say Defence begrudges use of its resources to deal with non-conventional security threats, or that its commitment to doing so has not increased in the years following September 11th. Rather, it is to make the point that the Department would not wish to see its capacity to defend Australia from military attack seriously eroded by such demands.

This reluctance and incapacity to use Australia's most valuable assets in meeting non-conventional security threats potentially leaves law enforcement short-changed in relation to some kinds of international challenges. However, given the rising profile of such issues in recent years, the law enforcement budget has risen dramatically in absolute terms and also in comparison with the Defence budget. For example, in 1999-2000, the budget for the AFP constituted only 1.4% of the Defence budget, whereas by 2005-06 the AFP budget constituted 4% of the Defence budget. The actual increase in the AFP budget over that period was from an

[48] Under the National Security Information (Criminal Proceedings) Amendment (Application) Bill 2005, some national security information would be allowed to be protected in court proceedings.
[49] *Defence 2000: Our Future Defence Force*, Australian Government, Department of Defence, Canberra, 2000, http://www.defence.gov.au/whitepaper/docs/WPAPER.PDF, p. VIII.

allocation of $249 million in 1999-2000 to $816 million in 2005-06.[50] Some of these additional funds have been used greatly to expand the network of AFP overseas liaison officers, increase cooperation with regional countries and increase numbers of sworn officers. However, a significant portion was also allocated to supporting specific government initiatives in the Solomon Islands, East Timor and PNG. Such initiatives in a general sense help to stabilise the regional environment. But they do not add significantly to the capacity of the AFP to deal with individual acts of transnational crime and terrorism.

Even given the rise in the AFP's budget both in absolute terms and *vis à vis* Defence, the organisation is still severely stressed in meeting the escalating expectations placed upon it, both in terms of its growing role in assisting Australia's foreign policy objectives and the escalating challenges posed by transnational crime and terrorism. This is but one of a number of anomalies and discontinuities that have become increasingly manifest since the end of the Cold War and in the context of the rapid change in threat perceptions resulting from September 11th.

The ICT Revolution and Australian Intelligence

The ICT revolution has enabled the construction of vast data streams capable of being merged, searched and analysed. These are available not only to decision makers, operations areas and intelligence agencies, but also the general public and media in the form of so-called 'open source information' (OSI). The ICT revolution also provides the capacity for all levels of organisations and operatives in different organisations to communicate vertically and horizontally in real time. It provides for the linking of these communications to information management and storage systems and to sensors capable of providing real time depiction of battle zones and other types of 'operational areas', such as public venues and public transport through CCTV, surveillance and other means. And finally, it provides for the capacity to interrogate, manage and assimilate these vast data holdings through 'knowledge management' tools. There are several implications for intelligence arising from these developments.

First, in terms of the policy-intelligence relationship, executives and policy makers through access to OSI are often able to know about events as soon as their intelligence subordinates know about them, and even sometimes before. As Berkowitz points out, this opens out significant competition for intelligence agencies.[51] In an open source environment, intelligence has become one of a number of competing information sources available to

[50] Based on budget papers for appropriations. The AFP data include community policing in the ACT.

[51] This was described by Bruce Berkowitz in 1996. See 'Information Age Intelligence', *Foreign Policy*, Summer 1996, pp. 35-50.

policy makers. According to Dupont, policy and command will to an extent be able to bypass and 'second guess' intelligence and structures may become flatter.[52] An example of the important role of OSI occurred when President Clinton's National Security Adviser, 'Sandy' Berger, reportedly informed the President only one hour before a deadline for an attack on Iraq in 1998 that Bagdad was offering a settlement – a detail he found out from CNN.[53]

As Treverton notes, however, OSI will not replace intelligence. Given the vast quantity and varying quality of OSI, intelligence will still be needed to sort, interpret and validate information. This validation will be needed with extreme rapidity and will involve a far more eclectic range of issues than during the Cold War.[54] In exercising this role, intelligence will need to marry secret information from SIGINT, human intelligence (HUMINT) and similar sources with OSI through knowledge management tools in order to leverage secret information from OSI and *vice versa*.

Intelligence will also be needed in presenting the longer term, strategic view. In fulfilling this role, it will use HUMINT and SIGINT and the other 'INTS' to interpret what Treverton refers to as 'mysteries'. According to Treverton, mysteries differ from 'puzzles' in that puzzles have already occurred and are 'knowable'.[55] A puzzle, for example, might be to derive an order of battle from an incomplete picture constructed from limited information. A mystery, on the other hand, might involve an analysis of how China might behave when it becomes rich and powerful. It is largely unknowable both because the Chinese leadership itself probably does not fully know the answer, and also because the outcome is dependent not just on China but also on how the West behaves towards it. To the extent that intentions are knowable and mysteries subject to interpretation, however, HUMINT and SIGINT are important tools in providing the necessary longer term, strategic view. These types of information acquisition take considerable resources and long periods of time to put in place and maintain and will always be the primary domain of intelligence services rather than open source providers.

A second transformation of the intelligence environment brought about by the ICT revolution is that the conceptual separation between command (policy), intelligence and operations is potentially radically undermined. In the classic form of this relationship, intelligence, at the direction of command, garners information from operations and other collection sources and provides analysis to command, which then develops 'policy' and directs operations accordingly. Following that, a whole series of new steps are

[52] See A Dupont, 'Intelligence for the twenty-first century', *Intelligence and National Security*, vol. 15, no. 4, Winter 2003, p. 25.
[53] Reported in Treverton, *op cit*, pp. 30-31.
[54] See Treverton, *Ibid*, pp. 20-61.
[55] See Treverton, *Ibid*, pp. 11-13.

taken in order to discern the effects of the operations already undertaken. Obviously, this traditional intelligence cycle, as originally set out by Sherman Kent, cannot be conducted in anything like real time.[56]

The ICT revolution enables all levels of this chain to communicate with all others in real time, however. It also sometimes enables a near real time picture of the 'battle space' to be constructed, especially by a power that is vastly superior to the enemy and controls the airspace. The highly complex pattern of communications that is produced by this capacity requires certain equally complex management tools if it is to be useful. Through various techniques, some of which are discussed below, use of these systems in turn results in a collapsing of the traditional intelligence cycle in a process in which both the individual steps and distinctive roles are merged. Several analytical concepts have emerged to describe and clarify this process.

Effects based operations (EBO – sometimes also known as effects based planning) was initially developed and used in the US Air Force and is defined in the following terms according to one Air Force publication:

> Effects-based operations (EBO) are . . . operations conceived and planned in a systems framework that considers [sic] the full range of direct, indirect, and cascading effects—effects that may, with different degrees of probability, be achieved by the application.[57]

Central to EBO is the idea of the *systems* nature of warfare. This is an environment that is constantly affected by our interventions and the interventions of the enemy and we need constantly to understand those effects in order to determine which intervention is most efficient in terms of achieving our goals. Further, we need to consider not just the immediate effects but also the 'cascading effects'. Finally, and most importantly, in deciding on a course of action we need to be mindful of the range of interventions available to us, and expected outcomes from those interventions. With that knowledge in hand, we then choose the most efficacious course of action in terms of our ultimate objective. Thus, in the case of the second Gulf war, a major objective was to cripple the communications system and leave the Iraqi army 'headless'. This was deemed the most efficient way to defeat the enemy with minimum losses. This initial defeat was successfully undertaken, but the EBO analysis evidently did not extend to the subsequent 'cascading' effects (what would happen next), to the detriment of the overall goal of the intervention.

[56] S Kent, *Strategic Intelligence for American World Policy*, Princeton University Press, New Jersey, 1971 – first published 1948.
[57] D F Fayette, 'Effects Based Operations: Application of new concepts, tactics, and software tools support the Air Force vision for effects-based operations', US Air Force Research Laboratory's Information Directorate, http://www.afrlhorizons.com/Briefs/June01/IF00015.html.

The concept of the 'OODA Loop' (Observe, Orient, Decide, Act) is in some respects similar to EBO, especially in its emphasis on the constantly shifting nature of warfare according to the effects of intervention and the consequent importance of 'feedback'. Its purpose is to enable decision makers to 'get inside' the enemy decision cycle and catch him off-guard. This in turn depends on a series of feedback events that are conducted in near real time and that short-circuit the step-by-step relationship of the traditional intelligence cycle.

EBO is very similar in concept to intelligence led policing (ILP). Both seek to be 'strategic' in their approach to solving problems and both are concerned with achieving the most efficient solution. In both cases the intelligence-policy separation is broken down in that the knowledge provided by intelligence also points to the solution. The idea of ILP is to use one's knowledge of crime to solve 'crime problems'. Instead of the old notion of investigating and prosecuting all crime as it occurs, ILP seeks to use a variety of means – some of them not necessarily based on prosecution outcomes – to target crime in the most efficient available manner. For example, intelligence may indicate that most crime in a location is perpetrated by half a dozen serial offenders. It may prove impossible, however, to get sufficient evidence to arrest and gaol them. One option under ILP would be to monitor them so closely that they would have no opportunity to offend. Eventually, rational choice theory would dictate that they would forego crime or go to another jurisdiction. Or at a simpler level, if intelligence shows that most violent crime revolves around a particular pub on Friday night, then that location can be saturated with policing to alleviate the problem.[58]

For both EBO and ILP, the key to success is the acquisition of intelligence by all as it is generated up and down the chain of command. Under EBO the pilot actually acquires the picture of the battle damage he inflicts and conveys it in real time. Under ILP, the police patrol car driver cannot simply drive around randomly to show a presence. He or she must do so with a view to passing through those areas where crime problems are to be found, both to interdict and deter crime and provide additional intelligence. In other words, intelligence is both generated at all levels and used at all levels, if not in real time, then close to it.

In the case of both EBO and ILP it is crucial that intelligence is derived from holistic, merged sources. It is this broader view that gives a picture not just

[58] Intelligence led policing frequently raises civil liberties concerns. For example, in some cases patrol cars are parked outside houses of 'known criminals' every morning just when the children leave for school; or a 'known criminal' can have his vehicle constantly stopped and his papers checked, and so on. However, in most of its manifestations it simply involves using devices like crime mapping better to target the law enforcement response to crime. Intelligence led policing exponents have also been accused of simply moving the problem elsewhere. To this accusation they reply that other jurisdictions are quite free to use similar methods.

of the 'battlefield' but also the environment surrounding the 'battlefield' – crucial to an understanding of the 'cascading' effects of any intervention. It is this holistic (and whole-of-government) notion of intelligence that deeply challenges the tightly contained AIC model.

ILP is heavily dependent on the ICT revolution, but not to the same extent as EBO. It would be possible to mount a credible ILP campaign using more traditional intelligence and research techniques. ILP allows for more time because it is not so dependent in the connectivity of weapons, sensors and decision-making in near real time as warfare. In this respect, ILP in its best form is equivalent to the concept of 'evidence based intervention' in medicine – a type of intervention that promotes efficacy based on knowledge of what works and at what cost, both in terms of 'upstream' and 'downstream' costs. It is, however, similar to EBO in that practitioners need a constant picture of the 'crime environment' and what is affecting it based on multiple databases and analytical tools such as merging and knowledge management of data, crime mapping and criminal network analysis tools. As with EBO, operations and the observance of operational effects are key components. This implies a change in the overall relationships between policy, intelligence and operations, with far more engagement between the three – a key point for the purposes of this paper.

Because they require considerable IT connectivity and integration between operating units (such as policy, intelligence and operations), methods like ILP and EBO are best applied at the agency level. In the sense of their underlying purpose of achieving strategic and efficacious intervention, however, they can also be effective at the whole-of-government level, but not necessarily in real time. But at the whole-of-government level, issues of management loom even larger than they do at the agency level.

In the Australian context, the difficulties with implementing such approaches on a whole-of-government basis are exacerbated by the fact that the AIC is charged with protecting highly sensitive national security secrets in the context of the 'cousins' and consequently sits like a 'hat' above the other intelligence agencies. This causes an artificial cut-off preventing better utilisation of data on a whole-of-government basis. The AIC, with the ONA at its apex, maintains the high ground as the filtration point for all high value intelligence into the government. But the AIC agencies are often ill-equipped to understand the full ramifications of the information and intelligence under consideration, and certainly not in real time. More especially, they are ill-equipped to place those different issues in any kind of priority. As occurred in the case of the so-called 'dirty dossier' in the UK, apex intelligence organisations like JIC, in their quest for brevity and political relevance, can

on occasion filter out the specific expert knowledge so necessary for a full understanding of complexity.[59]

A third set of implications of the ICT revolution relates to communications between agencies and access to data. If secure, real time communications can be established at all times, and if the intelligence outcome needs to be based as far as possible on holistic, and whole-of-government approaches (which is certainly one implication of the advent of non-conventional security issues as outlined above), then a number of questions follow.

First, who should, and who should not, have access to data that can be merged as a result of these technologies in order to provide synergism for intelligence information? In considering this issue, both privacy and security issues arise. Secondly, where is it most efficacious to terminate the boundary of those passing intelligence to the central database? And thirdly, what is the relationship, if any, between keeping data providers at the periphery informed of central policy considerations and their capacity to provide useful intelligence to what Flood refers to as the 'inner core' of the AIC?[60]

Let us take the last of these points first. It is axiomatic of sound intelligence practice that collectors do not collect and disseminate in a satisfactory way if they are unaware of what is developing around them and how it is affected by policy considerations. (This is equivalent to the 'orient' phase of the OODA loop). If operational collectors and reporters are isolated in this way, they do not know what best to collect to contribute from the periphery to the central effort. Moreover, what they do collect is often not passed on by intermediaries who themselves may be unaware of the policy context, contributing to the problem of 'stove-piping', which made a major contribution to the intelligence failure of September 11th. Finally, if intelligence officers at the operational level are isolated from the central policy context, they can misconstrue the way their intelligence is dealt with at the centre, sometimes with highly deleterious results. Such isolation from central policy may have been a factor in the case of Lt. Colonel Lance Collins.[61]

[59] Dr Jones, a foremost expert on WMD within the DIS, questioned figures in the 'dirty dossier' but was told by his superiors that they relied on intelligence too sensitive for him to see. The Butler Report comments that Jones should not have been denied access to a report concerning which he was best placed to provide expert commentary. Butler Report, *op cit*, pp. 137-9

[60] Flood Report, *op cit*, p. 76.

[61] In the view of the author, Collins' assertion that the Indonesian military (TNI) was complicit in a potential 'bloodbath' in the absence of UN or Australian military intervention prior to the act of determination in Timor was correct, and was proven to be so. However, the wider context for the decision by the government that it could not intervene despite the warnings from Collins and others (of which it was well aware), was determined by the policy decision that such intervention would likely have resulted in war with Indonesia and that this would be a worse outcome than the one that actually occurred. Had Collins been fully apprised of the government's thinking at

ICT itself can be used as a means to reduce some of the above problems, especially 'stove-piping'. It provides for interactivity of various databases, known as 'data fusion'. Provided adequate search engines and knowledge management tools are placed over the top of fused data, the mythical 'dots' of intelligence can better be connected. (It needs to be emphasised, however, that IT solutions can never be a complete substitution for adequate communication between human beings).

Data fusion in turn raises a whole set of subsidiary issues. These are evident when we examine attempts on the part of the US to deal with the problem of 'stove piping' in the aftermath of September 11th. The US attempted to deal with such problems in four main ways.

The first was to lump a whole range of authorities into one giant department, known as the Department of Homeland Security (DHS).[62] Within the DHS, the Directorate of Information Analysis and Infrastructure Protection draws on the amalgamated agencies that now comprise the DHS to maintain an 'all source' database on individuals. However, since the DHS does not include defence agencies or even key domestic agencies like the FBI, this is not a complete database by any means. Moreover, the perceived failures of the DHS in the aftermath of hurricane 'Katrina' are likely further to tarnish the already questionable reputation of the giant, cumbersome department.

Secondly, the US has attempted to improve agency coordination by setting up a cabinet-level position to oversight and coordinate the 15 agencies that constitute the US intelligence community.[63] This position, known as the Director of National Intelligence, reputedly has a budget oversight role over the agencies. In this it differs from the previous coordination arrangement, which involved the Director of Central Intelligence acting without budgetary authority.

A third approach, outside the scope of the DHS, but including elements from within that department, was the development of a 'fusion centre' similar in nature to Australia's NTAC. The Terrorist Threat Integration Centre (TTIC) was developed under the auspices of the CIA in 2003. It is designed to bring together personnel and data from the Department of Defense, the CIA, the FBI and DHS. It covers both domestic and foreign intelligence.

---

the point at which he felt himself to be in policy divergence with Defence in Canberra, it is possible that the subsequent unfortunate events may not have occurred.

[62] Made up of the US Customs Service, Immigration and Naturalization Service, Transport Security Administration, Federal Law Enforcement Training Center, Animal and Plant Health Inspection Service, and Office of Domestic Preparedness.

[63] These are the CIA, Air Force Intelligence, Army Intelligence, Navy Intelligence, DIA, Marine Corps Intelligence, NGIA, NRO, NSA, NI, FBI (National Security Division), DHS (CGI and IAIPD), DOE, DOS (INR) and Treasury.

Fusion centres such as the TTIC and NTAC can alleviate the jurisdictional, privacy and technical issues involved in total data fusion to a certain extent. They do this by having analysts from the involved agencies as 'brokers' who control access between the fusion centre and the participating agency. Thus the inter-face analyst will have access both ways across the firewalls around the fusion centre and the agency concerned and will 'broker' the exchange of information. In some cases, analysts can be joint members of all concerned agencies, thus removing the legal restraints on data access. This latter model is used for the AFP-led Joint Anti-terrorism Strike Forces, involving state and federal police.

While fusion centres can solve many problems, they do not provide genuine (automatic) data matching and real time data fusion. They are only as good as the respective individuals providing the interface. Moreover, both TTIC and NTAC apply only to terrorism intelligence and exclude the broadening range of non-conventional security threats daily confronting governments, such as the H5N1 flu strain, environmental issues like climate change and transnational crime.

A fourth approach in the US consisted of an attempt to 'fuse' information databases on an all-source basis into a 'data warehouse' and run search engines and other knowledge management tools over the top of those data. This was exemplified in the putative Total Information Awareness (TIA) project, established by the Pentagon in the aftermath of September 11th, but blocked by Congress on privacy grounds. (Indeed, such approaches are now becoming increasingly scrutinised by civil liberties organisations on the ground that they raise serious privacy issues.)[64] The TIA project was to involve genuine data merging and mining from all possible sources (including even library records). In this it differed from the individual agency, member-based system, such as the 'fusion centre' approach described above, which could be described as a 'federated' approach to data sharing.

Such data warehousing as attempted under the TIA need not *necessarily* imply breaches of privacy or other civil liberties. Another method of controlling data access is to fuse data, but continue to identify components of the fused data as belonging to the originating agency. Such data can then be accessed only according to the various sets of guidelines pertaining for those agencies that own it. For example, in a warehouse containing data from national security agencies, police, Customs and defence agencies, filtration tools could be devised that would allow each agency to view the others' data only according to the rules that apply, whether governed by security, legislative or other privacy concerns. At some point, however, there would need to be at least someone able to access all such fused data if any

[64] See the on-line journal *Privacy* and 'ACLU Questions Scope of "Intelligence Fusion Center" in Massachusetts', 11 May 2005, http://www.aclu.org/Privacy/Privacy.cfm?ID=18234&c=130, accessed 6 July 2005.

benefit were to be derived from the fusion of the data. Further, the finished product needs to be jointly managed downstream by participating agencies to ensure that breaches of their rules do not occur. In a sense, this model is a hybrid between a genuine data warehouse such as the TIA project and a 'fusion centre' of the type described above.

The British model for reform following the findings of the Butler Report does not go as far as the US model in creating fundamental change. In particular, it does not specifically deal with the need better to integrate data. Rather, it involves continuing with the JIC model for coordination and assessment (somewhat similar to the ONA) but bringing expertise into an expanded JIC in the hope that expert voices will not be lost. In addition, an individual within the JIC will be appointed with the specific role of challenging and checking all JIC findings.[65]

Data fusion is not the only issue at stake in the debate about the role of IT. Most communication networks also double as repositories of data. They do this through retained communications over time, retained product and the capacity to put search engines and other management tools over such data.

In the Australian context, the AIC is currently serviced by a highly secure, real time communications network known as AICNET. There are various other networks, both more extensive and more restricted in their ambit, but AICNET is the most important.[66] AICNET fulfils the dual function of a communications system and data warehouse, with certain in-built capabilities to sort information around specific topics and with communications, intelligence reports and information retained over time.

Other communications/data systems also exist outside the AIC. For example, the AFP case management system, the Police Real-time Online Management Information System (or PROMIS), is both a communications system with embedded, secure email, and a database for maintaining intelligence and investigations records and other intelligence product (managed as cases). Both AICNET and PROMIS contain systems to quarantine information within the total system, which is in turn 'firewalled' at the perimeter from outside access. In the case of PROMIS, there is also a facility to enable those who have access to exceptionally sensitive

[65] See a BBC News Report on the intelligence changes by Paul Reynolds 'Attitude vital to good intelligence', in *Voices of September 11th*, http://www.voices ofsept11.org/news/040405b.htm, accessed 27 September 2005.

[66] ASNET - share intelligence with state and territory government agencies; SATIN, connect to DFAT and international posts; CABNET, submission of Cabinet documents; AIMS, transfer of funding data with Finance; FedLink - Secure Inter-agency communication (From a paper delivered by Steve Alford at the 'Security in Government 2002' conference, hosted by the AG's Department, 10-12 April 2002).

information to know when any of the entities[67] upon which they are working receive a 'hit' from outside the quarantine. ASIO and other agencies also have their own communications-cum data systems.

Although the AIC is contained within the tightly firewalled AICNET (which is not further linked to systems such as PROMIS), the AIC does have some capacity to migrate outside information into AICNET, but not always in real time. For example, using DFAT cables from posts (which are compiled from information derived from all agencies represented at a particular post), NTAC fused product, and periodic debriefings by ONA, DIO and ASIO of police, customs officers and other operational agency officials, including those returning from overseas postings, AICNET can to an extent be populated with information from outside agencies.

Nevertheless, such remedies are only partial. Despite a mandated collection regime involving both the AIC and non-AIC agencies,[68] collection does not occur in real time and is serendipitous. Moreover, AICNET does not service a 'whole of government' client base. For example, only a tiny constituency within the AFP and Customs is privy to AICNET information. And even within the network, certain items originating from certain agencies are highly restricted. This means that, according to the dictum described above, non-AIC agencies cannot efficiently collect for the AIC. In making this point we need to note that highly classified information needs to be restricted not just to those with a need to know it, but also those appropriately cleared to see it. Clearances are costly and cannot be provided to all collectors of information.

On the other hand, with the end of the Cold War, the type of highly secretive information provided by the 'cousins' is ever less relevant to Australia's regional intelligence circumstances. (This, of course, could change, should another Cold War-like situation arise, say with China). Such intelligence was, for example, almost wholly irrelevant in providing support during the Sandline and the Solomon Islands crises. Even in the Timor crisis, Australia's own intelligence effort would probably have been the major provider of crucial information and intelligence. In the changed environment described in this paper, one increasingly comes to the view that the 'tail' of highly classified intelligence is wagging the 'dog' of whole-of-government requirements for intelligence.

[67] In police parlance the term 'entity' can refer not only to an individual but to other attributes of that individual such as a street address or phone number. This emphasis on entities in the wider sense enables connections to be made with crime scenes and individuals that would not otherwise be made.

[68] There are two sets of intelligence reporting requirements, which are adjusted periodically. These are the Foreign Intelligence Priority Directives (FIPD) and the Security Intelligence Priority Directives (SIPD).

Towards an Australian Model for Whole-of-Government Intelligence

We have argued in this article that throughout the period of rapidly changing intelligence environment between the end of the Cold War and today's post September 11th world, the traditional, hierarchical model for providing intelligence to the upper echelons of government persisted. Most security and defence information and intelligence of perceived value is still filtered through ONA or other agencies of the AIC. Because of the close connection between senior policy departments and the ONA, the advice given tends to be highly relevant to the perceived needs of government policy development when it is properly targeted, but not always inclusive of new threats and ground-level operational realities. That this is the case is illustrated both by the essentially unchanging structural nature of the AIC and by its performance, which has included some significant lapses that exemplify poor communications with operational agencies.

Structurally, there has been no major change in the organisation of Australian intelligence resources excepting the formation of the NTAC and the JTTU, which relate specifically to terrorism. The only other major change involving stronger communication with agencies outside the presently defined AIC consists of a recommendation to bring the AFP Commissioner permanently onto the Heads of Intelligence Agencies Meeting (HIAM), now re-named the Foreign Intelligence Coordination Committee (FICC) on the recommendation of the Flood Report.[69] Tellingly, the only real discussion of relations between the AIC and non-AIC agencies in the Flood Report related to a requirement for the AFP better to train its officers and develop systems to protect AIC intelligence.[70] No converse requirement was placed on the AIC in terms of its capacity to incorporate information and intelligence from operational agencies like the AFP.

The only matters raised about the ICT revolution in the Flood Report relate to the need to beef up the use of electronic communication *within* the AIC and the transfer of the OSI unit from DFAT to ONA. These issues are covered by a few short paragraphs.[71] Thus the issue of the definition of the AIC continues to dog the broader Australian intelligence enterprise and limit the uses that can be made of new technologies for communication, data sharing, data analysis and the management of the intelligence-policy interface.

---

[69] Flood, *op cit*, recommendation 7, p. 181.
[70] Flood, *Ibid*, p. 76.
[71] Flood, *Ibid*, recommendation 5 p. 180; recommendation 8(h), p.181. In the detailed discussion in Chapter 7, p. 161, Flood recommends that the FICC examine stronger IT connectivity within the intelligence community, but appears to define the community narrowly as 'the intelligence community (including ASIO)', suggesting all the operational departments and agencies should continue to be excluded.

The authors of the Flood Report may have reasonably assumed the dictum: 'if it ain't broke, don't fix it' – assuming it 'ain't broke'. This paper has argued otherwise. But criticism of the AIC flows easily and is not readily countered by an AIC membership bounden by law not to comment on the detail of intelligence. It is therefore incumbent on the critic to come up with a viable alternative. Such an alternative should protect the sensitive intelligence of Australia's allies, provide connectivity between the AIC and other intelligence using and producing agencies so a truly comprehensive intelligence picture can be provided to governments and other clients and, at the same time, preserve the type of tight intelligence presentation and coordination role for which ONA is justifiably noted. There may, indeed, be some arrangements that would get us some way along the path to meeting these objectives.

For example, ONA could be expanded (recommended by Flood in any case)[72] so that it fell into two broad categories, a smaller Strategic Intelligence Division (for state-on-state intelligence and highly sensitive intelligence sharing with the 'cousins') and a larger Security of Australia Division (for non-conventional threats, both as they impact domestically and internationally). Deputy Directors-General would head the two divisions. To reflect this change in emphasis, ONA could have its name changed to the Office of Australian Strategic Intelligence (OASI for short).[73] This would reflect both its domestic and foreign concerns – the two being increasingly difficult to separate in the globalised environment in which intelligence must operate. ASIO would remain the principal agency responsible for security intelligence gathering and analysis in the domestic sphere. Both the ASIO and ONA acts would require some amendment to enable this to happen.

ONA (or OASI) staff would for the first time consist of a truly professional intelligence service that would be drawn from, and interchangeable with, all using and producing departments and agencies, or their intelligence components where they are not specific intelligence agencies (including ASIO, ONA, DFAT, DIO, DSD, DIGO, AFP, ACC, DIMIA, Customs, Coastwatch, DOTARS, AQIS, DEFENCE and TREASURY/FINANCE). Clearances would be conducted and paid for jointly under the auspices of the office of Inspector General of Intelligence and Security (IGIS) or a central vetting agency housed in Attorney-General's Department.[74] Common professional standards, including promotion criteria and benchmarks would be set and maintained, also by the IGIS or AG's agency. The Flood Report makes a partial recommendation along these lines, but it relates only to staff within AIC agencies.

[72] Flood Report, *op cit*, Recommendation 4, p. 180.
[73] Flood recommended that ONA's name be changed to Australian Foreign Intelligence Assessment Agency, reflecting solely the foreign intelligence role. See Recommend.6, p. 180.
[74] A separate agency might be necessary in order to preserve the independence of the IGIS.

The widening of the AIC analysts' pool to include designated strategic analysts from operational agencies like Customs, the AFP, the ACC, Coastguard and DIMIA would have the effect of broadening the reach and knowledge base of the AIC and deepening the understanding on the part of AIC agencies of non-conventional security threats confronting the country, and *vice versa* for non-AIC agencies. This would occur because of the natural circulation of analysts between agencies, including OASI, and because of the existence of common levels of clearances.

The OASI would be serviced by an IT arrangement that would involve a mixture of the old AICNET arrangement in respect of the Strategic Intelligence Division and original AIC agencies and a federated data arrangement for the SOAD and non-original AIC agencies. This federated arrangement could involve merging where agency rules permitted or fusion centre-type arrangements where they did not, with analysts from respective agencies populating the SOAD to enable this to happen. The two databases so derived could be merged within the SID, at no threat to national security material, thus allowing for synergism between the national security intelligence and non-conventional security intelligence. Moreover, analysts from the SOAD could also look into SID data where cleared to do so. Those from agencies outside the original AIC could not where not cleared to do so. The communications network servicing the SOAD would have the capacity to reach down into the data of relevant departments and agencies, and SOAD product would also be more widely available within those agencies, through the presence of appropriately cleared and trustworthy strategic analysts. The current NTAC could be moved from ASIO into the Security of Australia Division, to reflect the whole-of-government nature of the data and personnel available. This system would thus be a combination of a full data fusion system with a federated system of data access and control.

Intelligence using departments and agencies could commission their broad strategic assessments (such as environmental scans) from OASI on a consultancy basis. OASI would contain analysts familiar with these fields because of the new inter-operable standards developed under the proposed arrangements. Further, where problems of national importance were identified that related closely to the work of departments or agencies outside the traditional AIC, the collection management and analytical processes could be 'commissioned' out to the most relevant agencies for the problem concerned, with the OASI retaining the coordination and decision-making role. For example, issues surrounding the H5N1 flu strain and its likely effect on Australia might be analysed jointly from the Department of Health and economic departments and agencies, which would be 'commissioned' for the task by OASI; or specific assessments on the impact of cyber crime and critical infrastructure might be run jointly by the AFP and DSD. OASI would retain ONA's current production, editorial and dissemination roles, thus ensuring that current high standards in these areas would be maintained.

More specific operational and strategic intelligence that did not have national import would continue to be run from within individual agencies on the present basis.

Tasking of the OASI and the setting of priorities would involve all concerned ministers, agencies and departments. SCONS would be the main tasking agency, on advice from relevant ministers and the NSC. SCONS would consist of all relevant agency and department heads, including Directors General of intelligence agencies. SCONS would in turn be advised of relevant issues by OASI, which would be well placed to give a whole of government perspective under the suggested arrangements. The HIAM (re-christened the FICC by Flood) would be folded into SCONS.

The great virtue of this system is that, while it would continue to provide the type of concise, readable, relevant intelligence that ONA is justly credited with, it would fully incorporate within that intelligence the wider operational intelligence and specific expertise available to executive and other agencies outside the current AIC. A depiction of this arrangement is given below (Figure 1).

Conclusion

The evolution of the environment in which Australian intelligence is required to operate has rapidly gathered pace since 1990. The end of the Cold War, changing nature of threat from state-on-state violence to non-conventional threat, and new tools introduced by the ICT revolution have each shaped the new environment. Globalisation has meant that the dichotomy between domestic and foreign intelligence is increasingly a false one. Yet despite this fundamentally altered operating environment, the architecture, and more important, the fundamental attitudes of the AIC have not changed in the thirty years since Justice Hope issued his first report.

The AIC remains tightly controlled, somewhat inward-looking, unable to benefit fully from the range of operational personnel who now work throughout Australia's region, largely inured to the possibilities offered by some important new technologies and increasingly unable to 'read the tealeaves' in Australia's near region. This defensive positioning enabled the AIC to maintain the confidence of allies in the context of the Cold War, but increasingly narrows the field of relevance within which the AIC operates.

The required changes are neither profound nor costly. Yet they would bring substantial benefits to the government and people of Australia and help position the country to cope with a rapidly evolving threat matrix into the twenty-first century.

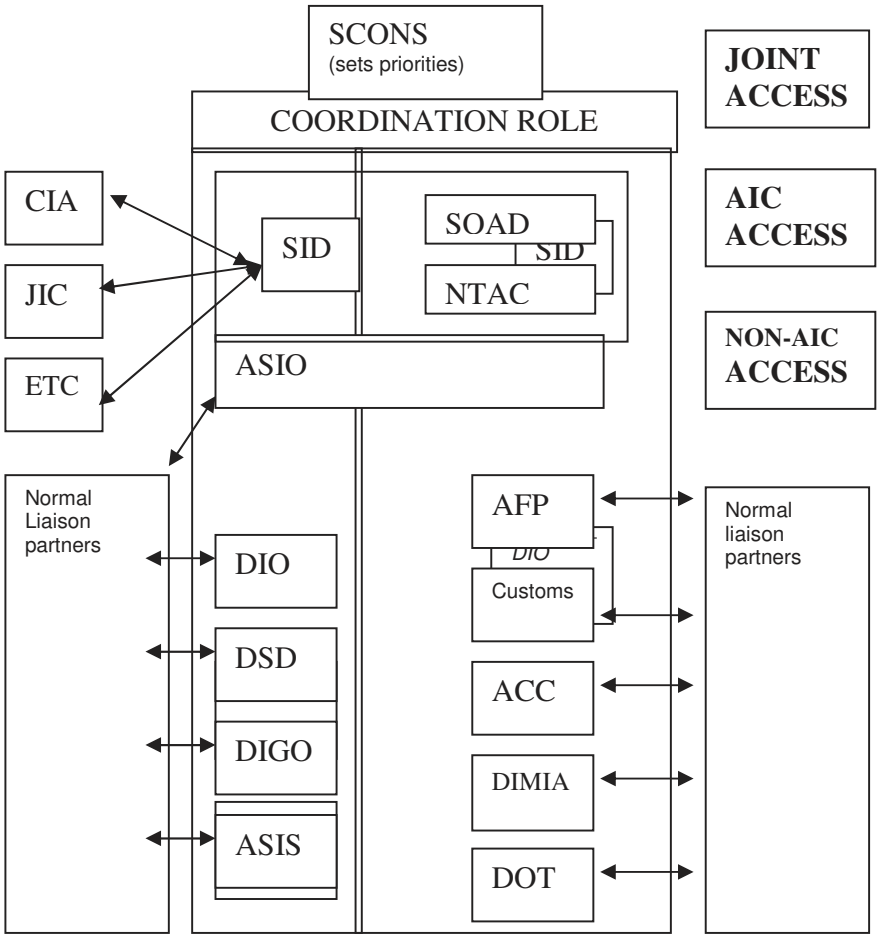

Figure 1

Sandy Gordon was awarded his BA from the University of Sydney in 1965 and his PhD from Cambridge University in 1976. He joined the Australian Public Service in 1977, subsequently working in the Office of National Assessments, AusAID and as Executive Director of the Asian Studies Council and Australian Literacy Council. In 1990 he became a Fellow at the Strategic and Defence Studies Centre, Australian National University, where he worked on South Asia and the Indian Ocean. In 1997 he was appointed head of intelligence in the AFP, a position he held until 2000. He then became Co-Chair of the Council for Security Cooperation in the Asia-Pacific Transnational Crime Working Group and a member of the National Expert Advisory Committee on Illicit Drugs. Between 2003 and 2005 he lectured on terrorism and transnational crime at the Australian Defence Force Academy, University of New South Wales. He is currently Associate Professor, Centre for Transnational Crime Prevention, University of Wollongong. thegordons@homemail.com.au.