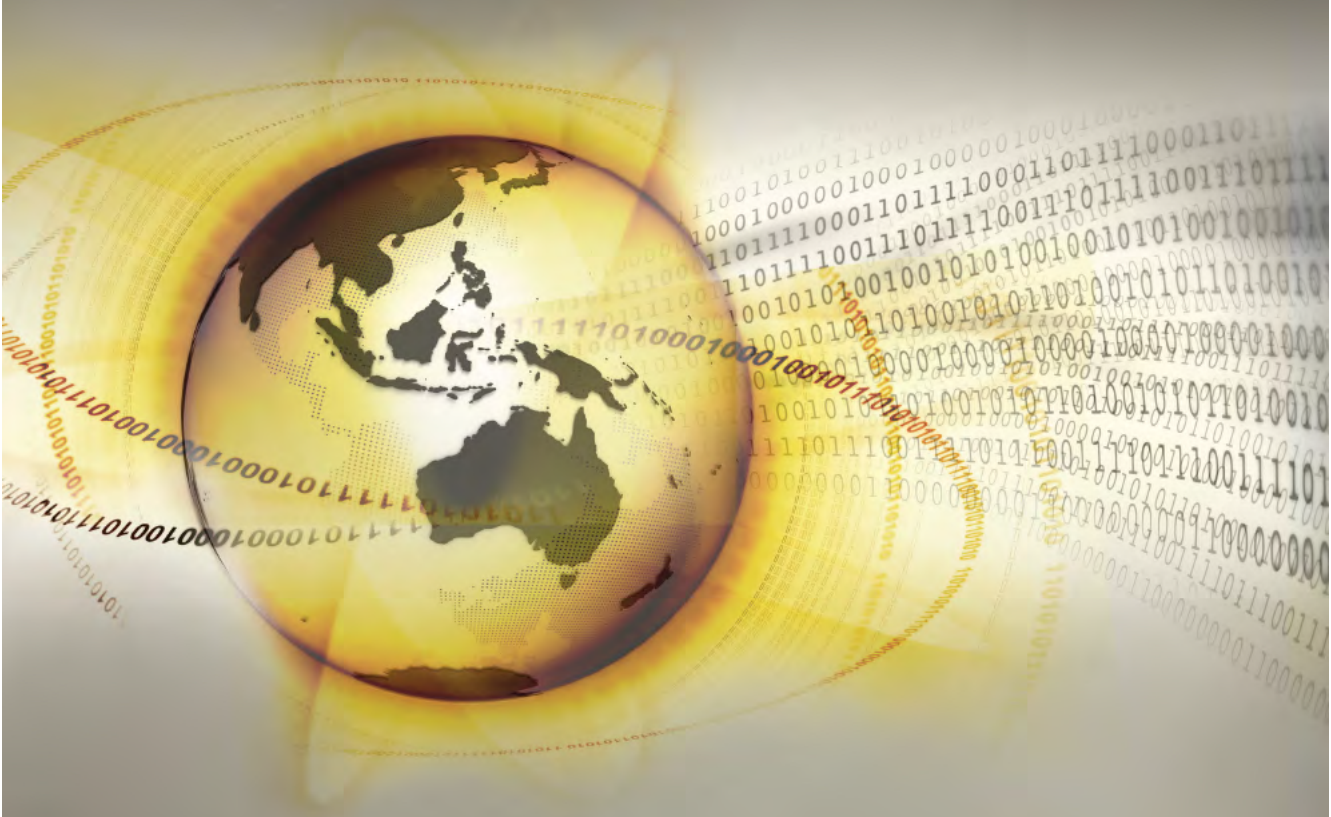
Australian Government

Independent Review of the Intelligence Community



2011

INDEPENDENT REVIEW OF THE INTELLIGENCE COMMUNITY REPORT

Robert Cornall AO Dr Rufus Black

2011

INDEPENDENT REVIEW OF THE INTELLIGENCE COMMUNITY REPORT

Robert Cornall AO Dr Rufus Black

ISBN 978-1-921739-72-9 (Hardcopy)
ISBN 978-1-921739-73-6 (PDF)
ISBN 978-1-921739-74-3 (RTF)

http://www.dpmc.gov.au/publications/iric/index.cfm

Enquires regarding the license and any use of this work are welcome at:
Department of the Prime Minister and Cabinet
PO Box 6500
CANBERRA ACT 2600
Tel: +61 2 6271 5111
Fax: +61 2 6271 5414
www.dpmc.gov.au

Australian Government

Independent Review of the Intelligence Community

16 November 2011

The Hon Julia Gillard MP
Prime Minister
Parliament House
CANBERRA

Dear Prime Minister

On 23 December 2010, you announced our appointment to undertake an Independent Review of the Intelligence Community.

Having completed the Review, we are pleased to now enclose an unclassified overview of our Report.

Our investigations into the Terms of Reference included a wide range of interviews with Ministers and former Ministers, Members of Parliament, relevant organisations and senior officials in Australia and in the United States, the United Kingdom, Canada and New Zealand. We also interviewed intelligence agencies and military officers engaged in operations in Afghanistan.

We called for submissions by public advertisement and received 38 submissions in all, including a very detailed submission from each intelligence agency.

Throughout the course of the Review, we received complete and courteous cooperation from the intelligence agencies and their officers.

The other people and organisations who made submissions or participated in interviews provided the Review with helpful contributions and useful insights into the performance of – and the issues confronting – Australia's intelligence agencies.

We were supported in our task by the members of the Review Secretariat and we acknowledge their professional, competent, conscientious and dedicated assistance.

Yours sincerely

Robert Cornall AO

Dr Rufus Black

This page intentionally left blank

Contents

This page intentionally left blank

Terms of Reference

The Independent Review of the Intelligence Community (IRIC) in 2011 will review the Australian Intelligence Community (AIC) in accordance with a recommendation of the Inquiry into Australian Intelligence Agencies (the Flood Inquiry) in 2004. The primary focus of this review will be the work of the six AIC agencies – Australian Security Intelligence Organisation (ASIO), the Australian Secret Intelligence Service (ASIS), the Defence Imagery and Geospatial Organisation (DIGO), the Defence Intelligence Organisation (DIO), the Defence Signals Directorate (DSD) and the Office of National Assessments (ONA).

The aim of the review is to address six key issues:

1. How well the intelligence community is positioned to support Australia's national interests, now and into the future;
2. Development of the intelligence community over the last decade, including implementation of intelligence-related reforms;
3. Working arrangements and relationships between the intelligence agencies and policy and operational areas of government;
4. Working arrangements and relationships between the intelligence agencies and their international partners;
5. Arrangements and practices within the intelligence community for collaborative work, including legislative arrangements; and
6. Level of resourcing dedicated to the intelligence community and apportionment of resources across the community, noting that any future proposals would need to be offset consistent with the Government's overall fiscal strategy.

The review will prepare findings and recommendations on the above issues and seek to provide a classified report to the Government around mid-year for its consideration in due course, as well as an accompanying unclassified version of that report.

The Department of the Prime Minister and Cabinet will establish a secretariat drawn from across the intelligence community and related agencies, as well as provide all other administrative support required. The review team will have full access to all material, including intelligence information and Cabinet documents, relevant to its examination. The heads of all relevant departments and agencies will ensure they and their staff co-operate fully with the review, and provide any requested assistance. Ministers will also be asked to meet with and assist the review team.

This page intentionally left blank

Introduction

This 2011 Independent Review of the Australian Intelligence Community was announced in the following media release issued by the Prime Minister on 23 December 2010:

> Prime Minister Julia Gillard today announced arrangements for an Independent Review of the Intelligence Community to start in early 2011.
>
> Intelligence plays a key role in preserving Australia's national security and supports a wide range of our national interests.
>
> The Prime Minister said the review will ensure Australia continues to have a well-coordinated, appropriately resourced and adaptable intelligence system that supports our national interests.
>
> The aim of the review is to ensure Australian intelligence agencies are working effectively together and are well positioned for challenges in a constantly evolving security environment.
>
> The Review will also consider working arrangements between intelligence agencies and their international partners.
>
> It will take into account the significant growth in the intelligence community's resources and capabilities over the past decade.
>
> The timing of the review meets a recommendation of the Inquiry into Australian Intelligence Agencies in 2004 by Mr Philip Flood AO, that the intelligence agencies undergo further external review every five to seven years. Funding for the Review was announced in the Budget in May this year.
>
> The 2011 Review will be led jointly by Mr Robert Cornall AO and Associate Professor Rufus Black.
>
> Mr Cornall has extensive experience at a high level in public administration, particularly as the Secretary of the Attorney-General's Department until his retirement in 2008.
>
> Associate Professor Black is the highly regarded Master of Ormond College at the University of Melbourne, and a notable ethicist, management consultant and theologian.
>
> The Review will produce its final report to the Government around the middle of 2011.

The Nature of the Review

It is worth making six introductory points about the nature of this Review.

It is the first comprehensive review of the Australian Intelligence Community since the 2004 Inquiry conducted by Mr Philip Flood AO[1]. There have of course been various reviews of individual agencies or aspects of their operation over the last seven years but no detailed consideration of the AIC as a whole.

Secondly, this Review is being conducted as a periodic review. It is not, as has usually been the case in the past, in response to a precipitating cause or event. As a result, the broad Terms of Reference require a general analysis and assessment of the intelligence community.

Thirdly, the primary focus of this Review is the work of the six agencies that have traditionally formed the Australian Intelligence Community – that is, the Office of National Assessments, the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Signals Directorate, the Defence Imagery and Geospatial Organisation and the Defence Intelligence Organisation.

However, while they are not directly the subject of this Review, a number of other agencies make significant intelligence contributions in their own areas of operation. Those agencies include military intelligence, the Australian Federal Police, the Australian Crime Commission, the Australian Customs and Border Protection Service, the Department of Foreign Affairs and Trade and the Department of Immigration and Citizenship.

The operational relationship and cooperation between the six core agencies and this wider group is important now and will become more important over time.

Fourthly, some significant policy changes have affected the intelligence community since 2004. A number of these changes were outlined in the National Security Statement delivered in Parliament on 4 December 2008. The changes include:

- The adoption of an all hazards approach to national security and the consequent increase in the number of agencies that comprise the national security community, and
- The appointment of a National Security Adviser and an increasing role for the Department of the Prime Minister and Cabinet in intelligence and national security matters.

Fifthly, the intelligence agencies have evolved substantially in the period covered by the Review. From agencies whose outputs were primarily directed to the development of policy, they now have a substantial operational role as well. The intelligence agencies have been integrally involved in supporting military operations, protecting our maritime borders, stopping weapons proliferation and thwarting terrorist activities in Australia and our region.

Sixthly, the Flood Inquiry had its primary focus on issues concerning the intelligence that had been provided to government on Iraq's weapons of mass destruction. Those issues had already received a great deal of public attention and had been the subject of a parliamentary inquiry. As a consequence of this general awareness, Mr Flood was able to publish a comprehensive unclassified version of his report.

This Review is different. It is not directed to a particular and well-known area of concern. The Terms of Reference called for a broad investigation into many highly classified or sensitive areas of the agencies' operations and resulted in detailed recommendations, which cannot be made public.

1 Note: the Flood Inquiry did not include the Australian Security Intelligence Organisation

Accordingly, this unclassified version of our Report provides a brief introduction to:

- The nature of intelligence
- What the government can reasonably expect from intelligence, and
- The Australian Intelligence Community.

Then we set out a general overview of the matters we considered and the conclusions we reached. However, in relation to topics where there has been public comment about broad policy questions – such as overall structure of the AIC or the balance between security and safeguards – we have set out our reasoning in more detail in appendices.

This page intentionally left blank

Chapter One

What is intelligence and what can reasonably be expected of it?

'Intelligence' conjures up many images. We set out in this Chapter what we mean by intelligence to help explain the approach and scope of the Review.

Government has come to expect much of intelligence, just as the public have come to expect much of government in providing for their security. So, in order to fairly assess the performance and preparedness of the intelligence community, we need to ask: What can government and the public reasonably expect from intelligence?

What is intelligence?

At the broadest level, intelligence has been defined either by the means it was obtained or by the outcomes it makes possible.

Those who have characterised it in terms of how it was obtained have used formulations like:

- 'Intelligence is covertly obtained information ... obtained without the authority of the government or group who "owns" the information'[2], and
- 'Secret intelligence is intelligence that others are seeking to prevent you from knowing, often with formidable security barriers and violent sanctions against those who cooperate with intelligence officers'[3].

However, those who have looked to what intelligence enables governments to do have used definitions like:

- 'Probably the simplest definition of intelligence is that it is useful information'[4]
- 'Intelligence is information gathered for policy makers in government which illuminates the choices open to them and enables them to exercise good judgment'[5]
- 'Intelligence is the collection and processing of that information about foreign countries and agents which is needed by a government for its foreign policy and national security'[6]
- 'The most basic purpose of intelligence is to improve the quality of decision making by reducing ignorance'[7]

2 Report of the Inquiry into Australian Intelligence Agencies (the Flood Report), July 2004, page 6
3 Sir David Omand, 'Securing the State', page 22
4 Allan Gyngell, 'The Challenges of Intelligence', speech to the Lowy Institute for International Policy, 30 March 2011
5 'Report to the President by the Commission on CIA Activities within the United States' (the Rockefeller Commission), June 1975, page 6
6 Martin T Bimfort, 'A definition of Intelligence', released by the CIA Historical Review Program, 18 September 1995
7 Sir David Omand, 'Securing the State', page 22

- 'Intelligence is information that has been analyzed and refined so that it is useful to policymakers in making decisions – specifically, decisions about potential threats to our national security'[8], and
- 'Intelligence is the systematic collection and processing of information about the enemy or adversaries into analyses, briefings and other products that are relevant and useful to military commanders'[9].

Given that a central task of this Review is to assess the performance of the Australian Intelligence Community, we decided to use an outcomes based definition of intelligence because we are concerned with evaluating the results the AIC has produced for government and its ability to continue to deliver them.

Therefore, we define intelligence as:

> Information that enables you to protect your interests or to maintain a valuable advantage in advancing your interests over those posing threats to them.

It is important to note that this definition does not distinguish between information that is obtained by clandestine means or through overt or publicly available sources. What matters is that the information confers an advantage through superior insight or the fact that you are in possession of information when others are not.

The definition does recognise that there is an offensive and defensive element to intelligence. It is about both obtaining information that confers an advantage and ensuring that your own information remains secure to protect your advantage.

Security and foreign intelligence

The notion that there is an offensive and defensive element to intelligence is reflected in the distinction between security and foreign intelligence:

- The term 'security' encompasses the protection of Australian people, interests and property at home and abroad[10], and
- A straight forward definition of 'foreign intelligence' is set out in section 5 of the *Telecommunications (Interception and Access) Act 1979* (Commonwealth). It says: 'Foreign intelligence means intelligence about the capabilities, intentions or activities of people or organisations outside Australia'. In that definition, 'foreign organisation means an organisation (including a government) outside Australia'.

We think that distinction remains a valuable one in limiting the realm and nature of different types of intelligence efforts.

Definitions by level of use

Intelligence confers advantage at a number of levels, which is reflected in the helpful distinction between:

- Strategic intelligence: the intelligence required to form strategy, policy and military plans and operations at the national and international level

8 www.fbi.gov/about-us/intelligence/defined

9 Australian Defence Force Academy: Oxford Companion to Australian Military History

10 See definitions of 'security' and 'foreign intelligence' in section 4 of the *Australian Security Intelligence Organisation Act 1979* (Commonwealth) and ASIO functions set out in section 17(1) of the Act

- Operational intelligence: the intelligence required for planning and conducting campaigns and major operations to accomplish strategic objectives within operational areas, and
- Tactical intelligence: the more immediate intelligence required in conducting operations.

These distinctions are important for this Review because Australia has seen the dramatic expansion of operational and tactical intelligence in the last 10 years.

Definitions referring to the method of collection

Intelligence is commonly further defined by the method of its collection. These definitions are of particular importance to Australia and its close allies because the structure of the community is built around these different methods of collection.

The categories set out below reflect the considerable sophistication and unique expertise that has developed around each of these disciplines.

One of the challenges this Review recognises in these definitions is the need to respect the distinctions between the different types of intelligence to preserve their distinctive capabilities but to bring all the information they generate together under one comprehensive definition and into a single outcome.

SIGINT – Signals Intelligence

Signals intelligence is derived from the interception of foreign communications. The Defence Signals Directorate is Australia's collector of foreign sigint.

HUMINT – Human Source Intelligence

Human intelligence is elicited from a human source by an intelligence officer or agent.

The Australian Secret Intelligence Service is Australia's principal collector of foreign humint. The Australian Security Intelligence Organisation collects humint in its security operations in Australia and overseas.

GEOINT – Geospatial Intelligence

Geospatial intelligence is derived from the collection and analysis of images and geospatial information about geographical features and events with reference to location and time:

- Imagery is typically gathered from satellites, reconnaissance aircraft, unmanned aerial vehicles and hand held photographic equipment on the ground. It can take the form of electro-optical, infrared and radar images or video, and
- Geospatial information refers to geographic and physical information in the form of maps, three dimensional virtual representations of landscapes in preparation for military operations and data about landscapes which can be used to guide weapons systems.

The Defence Imagery and Geospatial Organisation is Australia's collector of geoint.

Official information

Official information is information – often confidential in nature – that is non-covert but not publicly available. It is derived from liaison between Australian Ministers and officials and the ministers and officials of foreign governments or organisations or influential, informed individuals.

The most obvious and common source of official information is diplomatic reporting through the Department of Foreign Affairs and Trade.

Open source information

Open source information is useful information collected from non-covert published or publicly available sources including newspapers, journals, radio, television, the internet and so on.

Open source information is a valuable contributor to the process of assessing intelligence and forming judgments.

As the Flood Report noted in 2004:

> 'While intelligence information is important, and often vital, to assessment, it is normally not the main source of information used by intelligence assessment agencies. Open sources ... provide the greater part of the information available to the Australian Government'[11].

The Office of National Assessments has responsibility for Australia's Open Source Centre.

Assessors

The advantage intelligence delivers comes not only through what we collect but how it is analysed. Assessors of all the intelligence that is collected have the responsibility to create superior insights for decision makers. In Australia, that responsibility falls to the Office of National Assessments, the Defence Intelligence Organisation and, in the case of security intelligence, ASIO.

Counter-intelligence

Intelligence activity is not limited to collection and analysis of others' information.

We also gain an advantage in securing our own secrets and protecting the means, methods and people who obtain information for us. All of these activities fall under the definition of counter-intelligence.

What is it reasonable to expect from intelligence

Given the task of this Review is to assess the performance of the Australian Intelligence Community and its future preparedness, what is it reasonable for government and the public to expect?[12]

Some of the most senior members of the intelligence community around the world have been very concerned in recent times that expectations have become unrealistic.

In his nomination speech, the current Director of National Intelligence in the United States, James Clapper, said:

11 Flood Report, pages 6-7

12 We set out in greater detail what we think are reasonable expectations of intelligence in Appendix 1

> 'I think, too often, people assume that the intelligence community is equally adept at divining both secrets [information that is being kept from public knowledge] and mysteries [knowledge of what might happen in the future] ... but we are not'[13].

The Director General of the British Security Service explained this concern very clearly in a speech he made last year:

> 'In recent years we appear increasingly to have imported from the American media the assumption that terrorism is 100% preventable and any incident that is not prevented is seen as a culpable government failure. This is a nonsensical way to consider terrorist risk and only plays into the hands of the terrorist themselves. Risk can be managed and reduced but it cannot realistically be abolished and if we delude ourselves that it can we are setting ourselves up for a nasty disappointment'[14].

We share their concern. It is important that Australia has realistic expectations about what intelligence can deliver.

Secrets

It may be possible to discover what DNI Clapper called 'secrets', which are existing states of affairs such as how many naval vessels a country has or what a foreign leader's intentions are.

While secret information can confer great advantage, an intelligence community can advise government about the difficulty, cost and risk involved in trying to obtain those secrets and the probability of success. If government is prepared to face the difficulty, meet the cost and take the risk, then it is reasonable for government to expect that probability of success.

If we are to remain an open society, there are also some absolute limits to what we can know about our citizens' secret intentions. As a result, there could be lone individuals or small groups seeking to plan and carry out violent plots that will be very difficult to detect.

Mysteries

More substantially, there are limits to what we can know about the future, that is, what DNI Clapper called 'mysteries'. The more closed a society is, the harder it will be to predict its future. That is why many of the greatest intelligence surprises have come from the most closed societies.

It is not simply that high walls of secrecy make information hard to obtain. More importantly, when civil society is subjugated, we cannot know how it will operate when it is no longer repressed. It will be very hard to judge, for example, how well supported underground leaders might be when they come to public prominence or how ready individuals will be to risk their lives in protests.

We have to tailor our expectations of intelligence accordingly.

While there is much intelligence can do for us, on occasion terrorists will succeed and the world will change in ways that surprise and unsettle us. If we have had realistic expectations of what intelligence can do then, hopefully, we will also have invested in creating the capacity to meet the shocks societies will inevitably face.

13 Nomination of LTGEN James Clapper, Jr, Hearing before the Select Committee on Intelligence of the United States Senate, 20 July 2010, page 9

14 Address by Jonathan Evans to the Worshipful Company of Security Professionals, 18 September 2010

This page intentionally left blank

Chapter Two

The Australian Intelligence Community

The Review examined the community of six government agencies whose primary mission is to provide the government with intelligence. In this Chapter we provide a brief introduction to each agency.

Australian Secret Intelligence Service

ASIS was established on 13 May 1952 by Executive Direction[15]. ASIS was not publicly avowed until 25 October 1977, when Prime Minister Malcolm Fraser declared the agency's existence and functions following a recommendation by the first Hope Royal Commission.

Until late 2001, ASIS operated under a Government Directive handed down by the National Security Committee of Cabinet to the Director-General. On 29 October 2001, stemming from the Samuels-Codd Commission of Inquiry recommendations, the *Intelligence Services Act 2001* (Commonwealth) came into effect, replacing the Directive.

The Minister for Foreign Affairs has responsibility for ASIS. The Minister oversees ASIS activities through several mechanisms under the *Intelligence Services Act*, including the requirement for ASIS to obtain approvals and authorisations before engaging in particular activities.

ASIS's role is to provide a human intelligence capability and secret intelligence not readily available by other means to support and protect Australians and Australia's national interests.

ASIS has the following functions:

- Obtaining and distributing secret intelligence about the capabilities, intentions and activities of individuals or organisations outside Australia that may affect Australia's interests and the well-being of its citizens
- Undertaking counter-intelligence activities
- Liaising with intelligence or security services, or other authorities, of other countries, and
- Undertaking other activities as directed by the Minister, such as providing support to the Australian Defence Force and military operations.

Defence Signals Directorate

The forerunner of DSD, the Defence Signals Bureau, commenced operations in 1947. The Bureau's intelligence role was formally acknowledged by Prime Minister Malcolm Fraser in a 1977 statement to the House of

15 ASIS was initially established through the mechanism of Executive Council minutes which formally empowered the Australian Government, under sections 61 and 67 of the Constitution, to form a secret intelligence service

Representatives about the Hope Royal Commission. The Bureau was subsequently renamed the Defence Signals Directorate.

The Minister for Defence has responsibility for DSD.

DSD is now regulated by the *Intelligence Services Act 2001*. DSD's role is to provide signals intelligence and information security support and advice. Its mission statement is: 'Reveal their secrets. Protect our own'.

DSD's functions are set out in the *Intelligence Services Act* and include:

- Obtaining intelligence about the capabilities, intentions or activities of people or organisations outside Australia from intercepted signals and communicating that intelligence in accordance with the government's requirements
- Providing material, advice and other assistance to Commonwealth and State authorities on matters relating to the security and integrity of information that is processed, stored or communicated by electronic or similar means
- Providing assistance to the Defence Force in military operations and to cooperate with the Defence Force on intelligence matters, and
- Providing assistance to Commonwealth and State authorities in relation to cryptography, communication, computer and other specialised technologies and the performance by those authorities of search and rescue functions.

Defence Imagery and Geospatial Organisation

DIGO was established under a Cabinet Directive on 8 November 2000 by amalgamating the Australian Imagery Organisation and Directorate of Strategic Military Geographic Information, and the Defence Topographic Agency.

On 2 December 2005, DIGO came under the provisions of the amended *Intelligence Services Act 2001*.

The Minister for Defence has responsibility for DIGO. DIGO's role is to provide geospatial intelligence from imagery and other sources in support of Australia's defence and national interests.

DIGO's main functions are to:

- Provide geospatial intelligence to help meet Australia's foreign intelligence requirements
- Support Australian Defence Force operational, targeting, training and exercise requirements
- Support the national security functions of the Commonwealth and State authorities
- Provide unclassified geospatial services such as digital and hardcopy maps and tailored imagery
- Provide technical advice and assistance on the use of geospatial information and services
- Provide data and metadata standards for current and future Defence systems and platforms, and
- Provide assistance to authorities undertaking emergency response functions.

Australian Security Intelligence Organisation

ASIO was established in 1949 pursuant to a directive given by the Prime Minister to the first Director-General of Security, Justice G S Reed. ASIO operated on the basis of this charter until legislation passed in 1956 put ASIO on a statutory rather than executive basis.

ASIO's role is to advise the government of security threats to Australians and Australian interests at home and abroad. 'Security' has a specific meaning for ASIO. It is defined in the *Australian Security Intelligence Organisation Act 1979* (Commonwealth) as relating to espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and serious threats to Australia's border integrity.

In practical terms, ASIO's functions include the:

- Collection of intelligence through a wide range of means, including human sources and technical operations
- Assessment of intelligence and the provision of threat assessments to government
- Investigation and response to threats to security
- Provision of security assessments including for visa applicants and for access to classified information and security controlled areas
- Provision of protective security advice to government agencies and owners of critical infrastructure, and
- Collection of foreign intelligence in Australia, at the request of the Minister for Foreign Affairs or the Minister for Defence.

The Attorney-General has responsibility for ASIO.

Defence Intelligence Organisation

The forerunner of DIO, the Joint Intelligence Bureau, commenced operations in 1947. In 1970, JIB merged with the intelligence assessment elements of the three armed services to form the Joint Intelligence Organisation. That organisation developed to become DIO in 1990.

The Minister for Defence has responsibility for DIO. DIO's roles and functions are specified in a mandate approved by the Minister.

DIO is an assessment agency. It provides defence-related intelligence assessments, advice and services, primarily to the Minister for Defence, members of the Australian Defence Force, senior Defence decision-makers, Defence policy planners and senior leaders of the Australian Government.

DIO's role is to provide strategic level, all-source intelligence and advice to support the Defence of Australia and its interests.

DIO's principal tasks are to provide:

- Assessments, advice and services to support current and potential operations by the Australian Defence Force

- Assessments on the intent and military capabilities of countries and foreign non-state actors relevant to Australia's security environment
- Technical assessments on weapons systems, cyber threats and defence-related technologies, and
- Specialist advice to support whole of government strategies, including to counter proliferation and combat terrorism.

Office of National Assessments

ONA was established by the *Office of National Assessments Act 1977* (Commonwealth) as an independent body directly accountable to the Prime Minister. The Director-General of ONA is an independent statutory officer who is not subject to external direction on the content of ONA assessments.

ONA's role is to deepen Australia's capacity to act in the world in ways that serve the national interest by increasing government understanding of international developments.

ONA's functions include:

- Reporting and assessment of international matters that are of political, strategic or economic significance to Australia
- Coordination and evaluation of Australian foreign intelligence activities, and
- The systematic collection, analysis and research of open source material to support Australian and allied government agencies.

Chapter Three

The performance and future preparedness of the Australian Intelligence Community: An overview of the Review's findings

In accordance with its broad Terms of Reference, the Review

- Looked back to assess the intelligence agencies' performance as they have grown rapidly to meet the expanding security challenges of the 9/11 decade
- Looked forward to the new and additional security threats in the cyber world and the challenges posed by the evolution of a multi-polar world and the economic rise of our region, and
- Asked what the Australian Intelligence Community will need to do to meet these challenges in an age of growing demands and abundant information but constrained resources.

In undertaking this task, the Review inquired into the detailed operations of Australia's intelligence agencies and the way they work with each other, with the agencies in the broader National Security Community and with their international partners.

As a result, the Review Report contains a great deal of sensitive and secret information from many sources. That material is so intricately woven into all aspects of the classified Report it is not possible to simply delete it and publish what remains.

Instead, we have summarised the essential thrust of the Report's conclusions in this Chapter, omitting the parts which must be kept secret and the detailed recommendations which go to the heart of the intelligence agencies' capabilities, activities and working relationships.

The growing security challenges of the 9/11 decade

The terrorist attacks in the United States on 11 September 2001 marked the beginning of a new era of security challenges for Australia. The threat of terrorism has been the gravest challenge, with more than 100 Australians killed in attacks overseas.

When these terrorist attacks reached our neighbourhood, we realised we had to step up our effort even more. We increased our homeland security and joined with Indonesia and other partners to degrade the regional threat. Further afield, including twice in Afghanistan, we have supported the United States and other partners in their efforts to disrupt the wider global jihadist network.

Failed and fragile states closer to our shores also demanded attention. At the same time, our maritime borders were being compromised by people smugglers and proliferators of weapons of mass destruction were of increasing concern.

While the intelligence agencies' attention was largely focused on those issues, espionage and foreign interference had not gone away and disruptive cyber activity was growing rapidly.

How the Intelligence Community responded to Australia's new security environment

To play its part in meeting these challenges, the Australian Intelligence Community had to transform itself in a few short years from its primary task during the post-Cold War period of contributing to policy development to the dual role it has today. Now, intelligence agencies not only inform policy, they also support substantial security and military operations at home and abroad.

The principal features of that transformation were new laws and expanded powers, a rapid growth in human and financial resources and a new national security architecture.

The anti-terrorism laws which created terrorism offences and expanded the powers of intelligence and law enforcement agencies were forged through a vigorous national debate that ultimately led to bipartisan support in the Parliament. The result of that process of political negotiation is that the Review did not hear any substantial criticism of the balance in our anti-terrorism laws between the security of the community and individual privacy and other civil rights.

The most substantial growth in resources came in the areas of security intelligence and foreign human intelligence, which had been substantially scaled back in the post-Cold War environment.

Overall, the combined budgets of the intelligence agencies grew by $753 million from 2000 – 2010 at a compound annual growth rate of 14.6% a year to a total of $1.07 billion.

Australia's return on this intelligence investment has been impressive. As a nation, we now possess a new range of well tested intelligence capabilities. Those capabilities have made Australia and Australians far safer than they would otherwise have been and have also made significant contributions to the global security effort.

There have been many notable outcomes, which demonstrate the value of this capability to Australia, as illustrated by the following examples:

- *Counter-terrorism:* The Australian Intelligence Community has helped keep the Australian homeland safe from terrorist attacks for a decade despite a series of major plots. Those disrupted plots resulted in 38 prosecutions and 22 convictions. Other potential plots have not been allowed to develop thanks to more than 80 foreign nationals being prevented from coming to Australia on security grounds and more than 50 Australians being denied the opportunity to travel to train for, support or participate in, terrorist activities
- *Support to military operations:* In addition to its contributions to force protection, intelligence has been integral to ADF operations
- *Disrupting people smuggling:* The combined efforts of the intelligence agencies (cooperating with law enforcement agencies) have significantly reduced the number of irregular maritime arrivals who would otherwise have arrived in Australia over the last few years

- *Counter-proliferation:* A significant number of people who might have been involved with the proliferation of weapons of mass destruction have been denied entry to Australia through the combined efforts of ASIO, the Department of Foreign Affairs and Trade and the Defence Intelligence Organisation in screening visa applicants. In addition, DIO export assessments have contributed to the whole-of-government effort which has prevented materials that might have been used in the manufacture of weapons from reaching their intended destination
- *Counter-espionage:* Agencies, principally ASIO, have continued to focus on the enduring challenge posed by espionage directed against Australia and its interests. This focus has included the development of responses to counter increasingly sophisticated espionage techniques, such as the use of the internet for espionage purposes, and
- *Countering cyber threats:* Since its establishment in 2010, the Cyber Security Operations Centre has identified a significant number of cyber security incidents, involving a wide range of threat sources, seeking to exploit Australian public and private sector computer networks for sensitive information. In conjunction with government and industry partners, the CSOC has provided advice and assistance to mitigate these threats.

Australia's relationship with its international partners, especially long standing allies, has been central to building this important national capability and achieving these outcomes.

As a result of Australia's joint operations with our allies throughout the 9/11 decade, Australia's intelligence relationships are at a very high point.

For Australia these close relationships have provided an enormous dividend. We are able to access a great deal of the intelligence acquired by our partners through their considerable investment in intelligence capability. Access to partners' intelligence is a huge multiplier to the capabilities and effectiveness of our intelligence agencies.

To build and maintain the intelligence capability we need, it is critical that Australia continues to invest in these relationships, working closely with our partners and contributing our share of the combined international intelligence effort.

However, Australia's middle power interests increasingly require our intelligence agencies to obtain global coverage by strengthening or developing other key intelligence relationships outside the allied community.

A new era for intelligence: meeting the challenges of a middle power with global interests in a multi-polar, cyber world

Looking to the future, we are of the opinion that we are entering a new era for intelligence. Important geopolitical and technological changes, which have been underway for some time, have now reached a point of maturity that they demand more attention and capability.

The rise of countries in our region has been referred to as the dawning of the Asian Century. In particular, the economic growth of those countries has made them emerging world powers with increasing importance and impact.

The internet has maintained its extraordinary growth, expanding the cyber world to all corners of the globe and deep into daily life. The world has become dependent on it.

Australia's own globalisation has continued so that today we are a middle power with global interests.

All of these changes are taking place in what has now become an age of information abundance. There is a rising ocean of open source information and yet, at the same time, covert intelligence is increasingly difficult to obtain.

While recognising that terrorism, espionage, proliferation and people smuggling remain clear and present dangers, we need to build a stronger national capability to meet the challenges of the multi-polar and cyber worlds.

We also have to meet the government's expectation that, when issues affecting Australians arise beyond our region, often suddenly, the intelligence community can provide prompt insight to inform decisions.

Multi-polar world

Navigating our international relationships will be one of Australia's greatest strategic challenges in the coming decades. The Australian Intelligence Community will be called upon to support government policy and decision making in a rapidly changing, multi-polar world.

Cyber threats

There is trouble in cyberspace.

Government networks have been penetrated by cyber intrusions. Australian strategic commercial interests have already been subject to cyber exploitation and we are still seeing only a portion of the hostile cyber activity.

The United States and China have both publicly acknowledged the importance of cyber war fighting capability, state-supported hacking is becoming a national capability in some countries and organised crime is colonising the cyber domain.

Australia needs to consolidate and expand its capabilities to counter the cyber threat through the CSOC in the Defence Signals Directorate. DSD, along with its intelligence and policy agency partners, needs to continue to build its capability to:

- Protect Australian government systems and systems of national significance
- Assist other agencies to meet high end threats, and
- Support the development of government and private sector capability to meet the high volume of cyber threats they will need to manage.

It is important to remember that, while DSD is in the vanguard of modern cyber applications, the world as a whole is still at what has been called the T-model Ford stage of the internet.[16]

Middle power needs

While we need to significantly increase our focus on our region and cyber space, they are not the only areas requiring more attention.

As a middle power with substantial commercial interests and citizens spread around the globe, we need a cost effective capability to see further afield to identify and understand potentially volatile areas that could affect us.

16 The latter part of the sentence attributed to Fairfax CEO Greg Hywood in 'The Diary' , *The Australian*, 25 April 2011, page 27

War fighting capability

Australia also needs to keep its war fighting capability on a sound footing. We still live in a dangerous world. There are rising powers and simmering tensions in our region. Our neighbourhood has vulnerable states that may again need our assistance. To help, we will need military capabilities that are increasingly more dependent on intelligence, ranging from the information required to operate smart weapons through to the surveillance and understanding of the human terrain that makes tactical operations far safer and more effective.

In the course of the last decade, Australia has built the impressive intelligence capability required for modern conflicts. It is vital we retain and build that capability, not only because it does much to secure the effectiveness of military operations but also because it expands policy makers' options as to how they will respond.

Meeting the new security challenges in a time of constrained resources

The central challenge for the Australian Intelligence Community is to meet both our existing and expanding security challenges in an era of constrained resources.

Some have proposed that the community would be more effective and efficient if its structure were to change. They argue that maintaining the distinction between domestic security and foreign intelligence is artificial and hinders effectiveness in a globalised Information Age.

The original logic for the distinction between domestic security and foreign intelligence counters this argument. The higher obligations we have towards our own citizens are best safeguarded by ensuring all members of an intelligence agency who deal with our domestic sphere operate according to a single regulatory regime and with one consistent set of operational practices and culture. At the same time, our foreign intelligence agencies need ways of working that are founded on a broader licence to operate effectively and require different skills and training.

Our view is that this original logic is sound. The possible compromise of the protections this distinction affords to Australians could not be justified by any of the potential efficiency gains that might come from dismantling it.[17]

There are other opportunities to increase the efficiency and effectiveness of the AIC that should enable it to meet the security and intelligence challenges of this new era.

Improved priority setting, mission integration and intelligence distribution

Priority setting would be assisted by a more analytic approach that is better aligned with the government's all hazards approach to national security. Sharper, better defined priorities will aid resource allocations and provide a greater return on our intelligence effort.

The return on intelligence effort is also enhanced by how well intelligence missions are integrated. Fusion centres have been an important step towards greater integration. The lessons from these successful mission integration efforts need to be widely applied.

In relation to the distribution of intelligence, it is important for agencies to continue to regularly and rigorously assess the utility of their intelligence products to ensure they are tailored to meet the needs of senior decision makers and that the substantial effort that goes into them is therefore well invested.

17 In Appendix 2 we set in greater detail our logic for maintaining the current structure of the AIC

More efficient and rigorous performance evaluation

There is considerable reliance on self-assessment and some duplication in the current evaluation process.

A cleaner process is needed, involving collectors being evaluated by assessors or operational users, assessors being evaluated by their customers and the performance of the agencies as a whole being evaluated from outside the intelligence community.

Outside input to support innovation

Constant innovation will be required in the years ahead to meet the rising demands facing the community.

The perspectives of people outside the community who understand the challenges facing intelligence agencies are a source of innovation. While AIC agencies already have processes in place to obtain external information and advice, these sources of independent opinion are likely to become increasingly valuable, given the world of abundant information and the complex global environment in which the AIC is operating.

New strategies for managing intelligence collection in the age of abundant information

The AIC needs a clear strategy to manage the vast and constantly expanding volume of:

- Electronic information, and
- The more accessible human information now available thanks to the greater ease of travel and its lower cost.

All of the intelligence agencies should:

- Ensure that their staff are skilled in the use of open source information and have easy but secure access to open source terminals and tools, and
- Invest in developing those open source tools and techniques so we can do an even better job of efficiently generating insights out of the rising ocean of data.

For all the value of open source reporting, it has its limits. Just as in an earlier age, intelligence agencies' reliance on signals intelligence led to the degradation of human intelligence to the point of vulnerability, we have to be careful that the amount of information freely available in cyberspace does not tempt us to fall into the same trap.

One way to avoid or at least minimise this vulnerability is to ensure our diplomatic service is able to meet the growing demand for insightful reporting about the many countries and issues which are now of interest to Australia.

Finally, while modern technologies facilitate the collection of more useful open source information, those technologies are making covert human intelligence gathering more challenging. Careful planning and investment will be needed to avoid these challenges severely constraining covert efforts.

Continuing to enhance working relationships in the community

There has been a major transformation in how well the Australian Intelligence Community is working together.

Their working relationships are particularly strong at the leadership level and can be further enhanced through joint senior management and leadership training. At lower levels, where some issues remain, it is important that the practices which have helped with improved collaboration, including rotations through other agencies and secondments, continue to expand.

At the institutional level, the community should continue to review the various fusion arrangements it has established to ensure the lessons learnt are shared. As these arrangements grow, care will need to be taken to disband some of them as well when those fusion centres or other cooperative arrangements have completed their task or met their objectives.

Continuing to deepen the quality of working relationships with the wider national security community

The intelligence agencies play an important role supporting the operations of some other agencies in the expanded National Security Community, which includes law enforcement agencies, the Department of Foreign Affairs and Trade, the Department of Immigration and Citizenship and the Australian Customs and Border Protection Service.

While these operational relationships are working well, the intelligence agencies should continue with their efforts to improve the way they work with the broader National Security Community.

Some care needs to be taken that the broad thrust to develop a larger National Security Community does not lead to collaborative arrangements and meetings whose size and complexity compromises any gain in effectiveness or efficiency they might have been intended to achieve.

Continuing to safeguard liberty and privacy in a time of heightened security

In a free society, it always important to keep the safeguards of our liberty, privacy and other human rights under review to maintain the balance we have struck as a nation between these individual rights and our security as a community.

The Review believes the legal framework that enshrines that balance is sound and does not need any adjustment at present[18], while recognising that periodic amendments will be needed to ensure the purpose and intention of the legislation keeps pace with changes in the nature of the threat and a rapidly evolving, technical operating environment.

This balance is not just protected by law and the regulatory and oversight regimes that regulate and monitor agency conduct. It is also protected by the culture of each agency and the intelligence community as a whole.

Maintaining the culture that sustains the balance between security and liberty, especially after a period of dramatic AIC growth, will require continued attention.

The intelligence community presently has to deal with the non-state actors who live largely outside existing legal and ethical frameworks.

Australia should take an active role in international discussions about the evolution of those ethical and legal frameworks and their effect on intelligence agencies and the way they should operate.

18 In Appendix 3 we set our justification for this view more fully

In addition to those challenges, the international community will face new questions that will arise about the appropriate and justifiable use of technologies like unmanned aerial vehicles and the possible outcomes of cyber attacks (including the potential for disproportionate harm to civilian populations).

For all that intelligence has done and can do, there are real limits on intelligence in a free society in a complex world. There will be closed societies whose futures will surprise us and there will be small extremist cells and even lone actors who will be very difficult to detect or stop.

What will matter on those occasions is that we have a robust society and an agile national security community as ready to respond to those events as they have responded to challenges of the past decade.

Conclusion

In summary, the overall conclusions reached by the Review are:

- The intelligence community has grown substantially over the last ten years in response to increasing demand, mainly in relation to terrorism, fighting wars and countering espionage (including cyber attacks), proliferation of weapons of mass destruction and people smuggling
- The investment made in building up the intelligence agencies has been justified and rewarded with more capability and increased performance
- That capability and performance has enabled Australia's agencies to make an effective contribution as a member of the international intelligence partnerships and their relationships with those partners are at a very high point which some interviewees described as 'the strongest they have ever been'
- The investment made in the intelligence agencies has resulted in improved capability and performance in Australia but it also gains Australia access to intelligence from international partners (through its contribution to common intelligence objectives) which Australia could never acquire by itself
- The intelligence agencies are working well together. They understand the need to cooperate and are paying close attention to developing fusion centres and other cooperative working arrangements (such as the Counter-Terrorism Control Centre) which have been developed over the last few years and will continue to evolve in future
- The intelligence agencies are also beginning to work more effectively with the other members of the recently expanded National Security Community. This evolution will take time – as is the case with any requirement for a significant shift in corporate behaviour – and it should be focused on those areas of common activity where closer cooperation can produce better results. The Review did not detect any lack of willingness to further develop these cooperative working arrangements
- The principal new challenges for the next five years or so will be to better align the AIC's priorities with the new geo-political and technological realities facing Australia as a middle power with global interests.

We believe that this periodic review has been very useful for both government – in assessing the intelligence agencies' current performance and future challenges – and for the agencies themselves by providing a formal opportunity for them to assess their current situation.

APPENDIX 1

REASONABLE EXPECTATIONS OF INTELLIGENCE

What can the government reasonably expect the Australian Intelligence Community will be able to tell it?

This question comes into sharp focus when events come as a surprise. Most recently, uprisings in the Middle East give rise to the question: Why were these events not foreseen? Given the task of the Review to assess the relative performance of the AIC and the expectations government should have of it in the future, it is important to set out our basis for answering these questions.

Over the years, senior members of the intelligence community – both in Australia and overseas – have been at pains to point out the limits to what intelligence can do.

In a speech to the Lowy Institute, the Director-General of ONA quoted a former US intelligence officer who drew a distinction between puzzles and mysteries:

> 'Puzzles can be solved: they have answers which only need to be revealed – how many intercontinental ballistic missiles did the Soviet Union hold? But a mystery, Treverton says, "poses a question that has no definitive answer because the answer is contingent; it depends on a future interaction of many factors, known and unknown. A mystery", he says, "cannot be answered, it can only be framed, by identifying the critical factors and applying some sense of how they have interacted in the past and might interact in the future"'[19].

The question the Review has asked is: What determines whether something is theoretically knowable? To help make that distinction and to determine what are reasonable expectations of government, we distinguish between the expectations of what can and what cannot be known about existing and future states of affairs.

Existing states of affairs

Existing states of affairs – which range from facts like how many naval vessels a country has to what its leader's intentions are – are theoretically knowable. It may prove very expensive, difficult and time consuming or even practically impossible to obtain that knowledge. What is important is that, because the state of affairs exists, in theory it could be known.

With this type of information, the intelligence community should be able to advise government about the difficulty, cost, risks and probability of success of different strategies to obtain it. In these situations there are two reasonable expectations government can have:

- First, government can reasonably expect that the intelligence community will be able to provide it with a fair representation of the trade-offs involved in seeking to obtain the information about existing states of affairs, and
- Second, government can reasonably expect that the intelligence community will be able to undertake its collection and analytic efforts in line with the trade-offs it identifies.

However, this expectation is subject to a critical qualification. In an open society, there is an additional constraint on what can reasonably be expected. The civil and political freedoms of our open society (including the right to privacy) have to be respected unless there is evidence that an individual or group is planning harm of a sufficiently grave kind to justify the limitation of those freedoms.

19 Speech by Allan Gyngell to the Lowy Institute, 30 March 2011, page 9

Respecting those freedoms means that the state cannot seek to know the intentions of all individuals or of such a large number of them that it would be hard for any individual to escape detection by the state (as occurred in East Germany).

The state cannot begin by seeking to know the intentions of every individual who may have malign intent. It must begin by operating at the level of the established social system. Therefore, consistent with an open society, the state can seek to identify groups or movements that might pose a threat. If such threats can be demonstrated then the state can move to focus on individuals of concern within those groups or movements.

Practically, this approach means that it may be very difficult to detect and stop small groups or lone individuals who are not part of some larger movement or group planning to carry out a violent plot. It is possible that the intelligence agencies could detect those individuals but it is also quite possible that they would not. The harm such individuals could cause is the price of an open society.

Therefore, a government can broadly expect that an intelligence community resourced for the task will be able to identify:

- Groups and movements from which threats could emerge, and
- Individuals within these groups or movements intent on causing harm.

However, as with any existing state of affairs, what is reasonable in any particular case will depend on the trade-off the government is prepared to accept between the challenge, risk and cost of pursuing the target.

What it is not reasonable for a government committed to an open society to expect is that the intelligence community will be able to identify and stop all security threats.

The importance of not having a zero risk expectation is not only as a safeguard to being an open society but also to avoid unpleasant surprises, over-reaction and misplaced quests for accountability as the Director General of the British Security Service explained very clearly in a speech he made in 2010:

> 'Our aim is to reach a position of assurance where any threat is identified and action taken to disrupt it before any harm is done, and particularly before there is an imminent danger to the public. This is of course easier said than done, and will never be fully achievable, but it is the aim.
>
> 'It is interesting to note in this context that in the last ten years what might be called a "zero tolerance" attitude to terrorist risk in Great Britain has become more widespread. While it has always been the case that the authorities have made every effort to prevent terrorist attacks, it used to be accepted as part of everyday life that sometimes the terrorists would get lucky and there would be an attack. In recent years we appear increasingly to have imported from the American media the assumption that terrorism is 100% preventable and any incident that is not prevented is seen as a culpable government failure. This is a nonsensical way to consider terrorist risk and only plays into the hands of the terrorist themselves. Risk can be managed and reduced but it cannot realistically be abolished and if we delude ourselves that it can we are setting ourselves up for a nasty disappointment'[20].

20 Address by Jonathan Evans to the Worshipful Company of Security Professionals, 18 September 2010

Future states of affairs

When it comes to future states of affairs, a very helpful approach can be built on the analysis of Nassim Taleb – author of 'The Black Swan' – who is particularly noted for his analysis of what can and cannot be known and predicted. In a recent article with Mark Blyth in *Foreign Affairs,* Mr Taleb addressed the question of what intelligence can know.

Nassim Taleb's analysis is founded on the following fundamental distinction:

> 'Humans simultaneously inhabit two systems: the linear and the complex. The linear domain is characterised by its predictability and the low degree of interaction among its components, which allows the use of mathematical methods that make forecasts reliable. In complex systems, there is an absence of visible causal links between the elements, masking a high degree of interdependence and extremely low predictability'[21].

When it comes to future states of affairs that are in the linear domain – for example, what a small terrorist cell is plotting to do next week – the expectation is essentially the same as with existing states of affairs. The key difference to existing states of affairs is that the intelligence community has to add its advice to an assessment of the probability that events will unfold as anticipated.

What is knowable about future states of affairs that belong to the domain of complex systems is a very different question. Mr Taleb's analysis is very helpful because it highlights that the extent to which the future is knowable is dependent on how open a society is.

Where a society is open – in other words, where there is a high level of civil and political freedoms including freedom of speech and association and the rule of law – it is possible to observe and map how the social, political and economic system works and, therefore, to form some conclusions about the likely directions of that society.

In closed societies – repressive states such as totalitarian dictatorships, theocracies and autocratic monarchies – the system is hidden. For example, the size and even the existence of opposition groups may be very veiled. It will be unknown how many citizens would join any movement. It is possible to speculate about such situations but such speculation will have high degrees of uncertainty attached to it and may prove very wide of the mark if there are social dynamics that are not visible or even in existence because of the level of repression.

These highly constrained states appear stable when, in fact, they may be extremely fragile and volatile. In the words of Taleb and Blyth:

> 'Complex systems that have artificially suppressed volatility tend to become extremely fragile, while at the same time exhibiting no visible risks'.

With such fragility, it will be unknowable what exactly will tip the system over the edge, as we saw very clearly with events that triggered the Arab Spring.

So it is not reasonable for government to expect the intelligence community to predict the timing, cause or nature of events like the Arab Spring or the collapse of the Soviet bloc. However, what government can reasonably expect is for the intelligence community to provide advice about:

21 Nassim Nicholas Taleb and Mark Blyth, 'The Black Swan of Cairo: How Suppressing Volatility Makes the World Less Predictable and More Dangerous', *Foreign Affairs*, Volume 90, No 3, pages 35–36

- The degree of volatility – for example, the AIC should be able to provide warnings to government about countries that are particularly volatile
- What factors would be likely to increase the volatility – for example, domestic pressures (such as more repressive measures) or outside influences (such as a rise in food prices or external attack), and
- What would make the society more knowable – for example, AIC agencies should be able to identify factors that would enable intelligence officers to better inform the government about the system, such as the rise of the free press.

Finally, reasonable expectations of intelligence change when a closed system starts to transition to an open society.

Initially, the government will need to look to open source reporting while the AIC develops assessments about the society and how it operates. However, as the society begins to operate, it will be possible for the AIC to provide more accurate and long-term assessments. Agencies should then be able to make assessments about individual groups and power balances and how they might play out.

While it is important to have a clear framework for what can reasonably be expected of the intelligence community, it is important to recognise that, as the Rockefeller Commission found in 1995:

> 'Good intelligence will not necessarily lead to wise policy choices. But without sound intelligence, national policy decisions and actions cannot effectively respond to actual conditions and reflect the best national interest or adequately protect our national security'[22].

Intelligence reports provide information and intelligence assessments offer judgments based on the best information then available to assist decision makers. But intelligence is only one factor decision makers take into account in making decisions.

Other factors include government policy, competing demands, legal and international obligations and so on, together with the decision maker's own judgment about the issue under consideration.

Availability of intelligence

Generally speaking, intelligence was historically well hidden and hard to get.

One of the major changes affecting intelligence agencies today is the ready availability of huge amounts of information which would previously have been difficult to obtain or simply not available.

Two factors contributing to this situation are the successful collection of sigint and the evolution of the internet.

It has been said that this new information environment requires flexibility in intelligence collection and a major shift from analysing what has been collected to analysing what to collect:

> 'We need to make tough decisions about which haystacks deserve to be scrutinised for the needles that can hurt us most. And we know in this information age that there are endless haystacks everywhere'[23].

22 'Report to the President by the Commission on CIA Activities within the United States', June 1975, page 2
23 Porter J Goss quoted in 'Strategic Intelligence, Volume 2', page 136

In 2004, the Flood Report defined intelligence as covertly obtained information. Open source information was a supplement for assessors. In 2011, the Director-General of ONA defined intelligence more broadly as useful information irrespective of source.

Arguments can be made in support of both statements, but they illustrate the major shift in the availability of valuable information that we believe will have a significant impact on our intelligence agencies over the next five to seven years.

That shift also highlights the fact that any helpful definition of intelligence has to go well beyond the collection and dissemination of useful information. Intelligence has to be clearly linked to the needs of individual customers and tailored for the purposes to which they can apply it. Otherwise, the recipients of intelligence reports will be overwhelmed by the volume of material they receive which will effectively reduce or even negate its ultimate usefulness for them.

APPENDIX 2

THE STRUCTURE OF THE AUSTRALIAN INTELLIGENCE COMMUNITY

The organisational structure of the Australian Intelligence Community has been based upon two principles designed to ensure its integrity, objectivity and effectiveness:

- The separation of what can be broadly categorised as collection agencies and analytic agencies: Collection focused agencies do make analytic contributions, undertake analysis to guide their collection and use other sources in this analytic work. The important point about this distinction is that there is a second agency whose exclusive task is to apply its specialist analytic capabilities to all sources of information and to do this work at one step removed from the collection effort, and
- The separation of security and foreign intelligence efforts.

The one exception to the operation of these principles is the Australian Security Intelligence Organisation. ASIO:

- Conducts its security intelligence operations principally in Australia but also overseas, and
- Collects and assesses intelligence on security issues.

The rationale for this exception is that threats to Australia's security can arise at home or abroad and separating the collection of security intelligence could compromise ASIO's central operational tasks, far outweighing any gain in the objectivity of its assessments.

It has been said that the structure and operation of our intelligence agencies reflects an out-of-date Cold War model. This Review does not agree with that opinion. We consider that the original logic for the current arrangements remains strong and there is no need for any change in the basic structure of the Australian Intelligence Community.

Separating collection from assessment

The separation between intelligence collection and assessment accords with the recommendations made in the Hope Royal Commission on Intelligence and Security and has stood the test of time. The Royal Commissioner found that, if intelligence assessments are to be accepted as objective, 'intelligence producers and the intelligence assessment process must be independent and be seen to be independent'[24].

Justice Hope said:

> 'The national assessment organisation should be separate from the collection agencies. The appearance and the dangers of a large, all-embracing central secret intelligence organisation, with collectors and assessors tending to support each other within the enclosed confines of the organisation must be avoided. The acceptability of assessments produced by such an agency could well be reduced, and people of high calibre might be deterred from association with the new assessment organisation'[25].

We accept the soundness of Justice Hope's arguments and believe that they are as applicable today as they were at the time of his Royal Commission.

24 Royal Commission on Intelligence and Security, Third Report, page 10
25 Royal Commission on Intelligence and Security, Third Report, pages 120-121

While different options are available for structuring this community, we accept that the optimal approach for Australia in managing its security machinery, given its federal structure and the history and culture of our particular government agencies, is likely to be based on a number of smaller, nimble, well connected organisations rather than fewer large organisations.

We also argue that there is considerable advantage in the structure of the Australian Intelligence Community agencies aligning well with our international counterparts. The similarity in their activities, functions and responsibilities facilitates joint operations, knowledge and capability transfers, effective staff exchanges and the embedding of liaison officers with similar training, skills and tradecraft. Given how important this collaboration is to the overall effectiveness of our intelligence effort, there is significant merit in retaining a structure that meshes neatly with our major intelligence partners.

Separation of domestic security intelligence and foreign intelligence

Some people argue that, in the globalised Information Age, it is artificial and hinders effectiveness to maintain the distinction between domestic security and foreign intelligence.

Justice Hope set out the original justification for this distinction very clearly when he wrote:

> 'The domestic collection capacity should be institutionally separate from the foreign collectors. The constraints within which the domestic agency should and must work, and its obligations of propriety, are fundamentally different from those of the foreign agencies. The demarcation should not be blurred, or be seen to be blurred'[26].

Today, as a result, Australia's foreign intelligence collectors are subject to different regulatory regimes than ASIO in its security functions. While there are effective oversight and authorisation arrangements in place that regulate the foreign intelligence agencies, those agencies are not subject to the more stringent legislative regime appropriate to ASIO's security activities.

As a general proposition, this Review is of the opinion that it would unnecessarily complicate the activities of a foreign intelligence agency and its legal compliance if it was to have security intelligence powers and functions comparable to ASIO's powers and functions in addition to its existing foreign intelligence responsibilities.

Equally, it is important to the protection of the rights of Australians that ASIO's culture and practices are shaped by an unambiguous legal and ethical framework which balances individual rights with national security concerns.

Ultimately, the important point of the domestic security and foreign intelligence distinction is not to do with the sphere of operation. It is based on the fact that significant rights and protections are afforded to citizens, residents and the general public in Australia and that different checks and balances apply to the security and foreign intelligence regimes.

Therefore, even if over time technology and globalisation require a weakening or elimination of the distinction between spheres of operation, the basic principles that separate agencies dealing with security and intelligence concerning Australian citizens and agencies dealing with citizens of other countries remain sound.

26 Hope Report, page 121

Other means to achieve more effective integration

The only – or at least the principal – remaining purpose in merging or restructuring agencies must be to obtain more effective and efficient performance of their functions. However, this outcome can be achieved by other means.

For example, it has been said that structures are one thing, how well they are joined up and work together is another. What is needed is to develop and build on proposals for more effective coordination among agencies, and to identify and address any legislative, technical or cultural obstacles to the integrated delivery of intelligence and security.

A similar conclusion was reached by Elaine Kamarck of the John F Kennedy School of Government at Harvard University in an article she wrote about the American experience with homeland security entitled 'Applying 21st Century Government to the Challenge of Homeland Security'. Ms Kamarck said:

> 'The initial instinct to create one agency to deal with a problem as broad as homeland security is inadequate to the task at hand[27]... The problem of homeland security ... does not fit in one box. To the student of 21st century government, the question is not "Where do the boxes fit on the chart?" but "How do they operate and how do they communicate with each other"' [28]?

Over the last few years, the intelligence agencies have conscientiously worked to achieve more coordinated intelligence outcomes within their existing structures by, among other things, the development of coordination or cooperation centres, shared training and facilities and so on.

Some brief details of three examples of this coordination and cooperation are set out below. They are the Counter-Terrorism Control Centre, the Cyber Security Operations Centre and the National Threat Assessment Centre.

Counter-Terrorism Control Centre

The CTCC was established in accordance with the 2010 Counter-Terrorism White Paper to coordinate terrorism intelligence and investigative activities at the operational and tactical level.

The CTCC is responsible for:

- Setting and managing counter-terrorism priorities
- Identifying intelligence requirements, and
- Ensuring the processes of collecting and distributing CT information are fully harmonised and effective.

The CTCC has the following members: ASIO (Chair), ASIS, DSD, DIGO and the AFP. It is located within ASIO.

27 Elaine Kamarck, John F Kennedy School of Government, Harvard University, 'Applying 21st Century Government to the Challenge of Homeland Security' June 2002, page 19

28 Elaine Kamarck, page 20

Cyber Security Operations Centre

The CSOC commenced operation within DSD in January 2010. It coordinates and assists with operational responses to cyber events of national importance. The Centre provides government with a consolidated understanding of the cyber threat through its intrusion detection, analytic and threat assessment capabilities.

The CSOC will in due course include a continuously staffed watch office and analysis team, which has the following members: DSD (lead agency), the ADF, DIO, ASIO, the AFP, DSTO and the Attorney-General's Department.

National Threat Assessment Centre

The NTAC is a 24/7 threat analysis and assessment centre set up in ASIO in 2003.

The NTAC analyses terrorist threats to Australian interests overseas and terrorist threats and threats from violent protests in Australia. The Centre provides threat assessments and country reports on the planning of attacks abroad – which informs DFAT travel advisories – and threats to high office holders and significant events to inform protective security measures.

The Centre, which is chaired by ASIO, comprises all AIC members plus the Department of Foreign Affairs and Trade, the AFP, the Office of Transport Security and the NSW Police.

There have also been improvements in IT connectivity and the sharing of corporate and back office functions between the three Defence intelligence agencies along with a number of other initiatives.

As a result of these considerations, this Review is of the opinion that there is no need to consider any significant restructure of the existing agencies at present although the agencies will have to consider carefully how they will adapt in response to the future challenges they face within those existing structures and cooperation arrangements.

APPENDIX 3

INTELLIGENCE, OVERSIGHT, SAFEGUARDS AND THE LAW

The terrorist attacks in the United States on 11 September 2001 marked the start of a decade of legislation creating new terrorism offences and conferring new powers – particularly on ASIO and the Australian Federal Police – to deal with terrorism.

A number of these laws were controversial. They prompted wide public discussion and debate about what were seen by some as a conflict between individual rights and the entitlement of the community to live in safety.

The Review has considered the anti-terrorism laws and related legislation as part of its investigation into how the intelligence community is positioned to support Australia's national interests now and into the future.

Legislative balance

The resolution of the perceived conflict between individual and community rights was not found in rejecting the proposed legislation but in establishing the appropriate balance between the two competing points of view.

The process of resolution in the Parliament often involved extensive negotiation between the Government and the Opposition. In some cases, significant amendments were made to draft bills before they were acceptable to both major parties.

As a result of those negotiations, all of the significant anti-terrorism and related Acts adopted since 2001 were passed with the support of Government and Opposition and there are many examples of Ministers and Shadow Ministers saying: 'We think we have got the balance right'.

We believe this process is a good example of the Parliament establishing the wider consensus that strong democracies obtain when an important adjustment is sought in the balance of rights. The strength of the broad social consensus and solidarity we have established about the new balance is itself a bulwark against those forces whose goal is instability.

Perhaps further evidence of the success of this process is that none of the submissions to this Review argued that the balance struck in the anti-terrorism laws should be substantially amended.

Nonetheless, the Review reflected on the balance. We came to the conclusion that the balance remains right for the future we face. Some of the arguments put forward in support of the current anti-terrorism and related laws are particularly persuasive:

- The aim of the laws is to protect the safety of the community as a whole and, in the process, protect the rights of individuals within society
- That aim is consistent with the Universal Declaration of Human Rights which states in Article 3 that: 'Every person has the right to life, liberty and security of the person', and
- Individual rights have to sit comfortably with this overriding human right to which everyone in the community is entitled.

These points were made very eloquently by Irwin Cotler, a leading human rights lawyer, when he was Attorney-General of Canada. Mr Cotler described counter-terrorism law and policy as the promotion and protection of both security and human rights. He said:

> 'Terrorism constitutes a fundamental assault both on the security of a democracy – indeed, on the peace and security of our hemisphere – as well as an assault on the most fundamental of rights – the rights to life, liberty and the security of the person. Accordingly, counter-terrorism involves the protection of both the security of a democracy – including the protection of international peace and security – and the protection of the most fundamental of our rights'[29].

Mr Cotler described those most fundamental rights as the right to life, liberty and security of the person[30] and the collective right to peace.

Safeguards

In reaching our conclusion that the balance between security and other rights is sound, we took careful note of the significant safeguards that have been built into the anti-terrorism laws.

One person consulted during the Review stressed that, while the laws contained strong provisions and some of them have not yet been required in operations, if the laws are needed in future they will be needed immediately.

Accordingly, the safeguard when granting strong powers to intelligence agencies and police forces is to ensure that there is strong oversight and accountability.

A number of safeguards regulate or are built into Australia's anti-terrorism laws and their application. They include:

- General oversight by Ministers of intelligence agencies within their portfolios
- The requirement for specific ministerial approval or authorisation before a number of actions can be taken by particular agencies
- Oversight by the Inspector-General of Intelligence and Security
- Oversight by the Parliamentary Joint Committee on Intelligence and Security
- Oversight by the courts if the legality of a particular action is challenged, and
- Internal training, supervision, monitoring compliance with corporate directions and policies with a strong emphasis on adhering to ethical standards.

Ministerial approval or authorisation

In addition to general ministerial oversight of agencies within their portfolio, the following examples provide illustrations of the requirement for ministerial approval or authorisation:

- ASIO must obtain a warrant from the Attorney-General to exercise its special powers (to enter and search premises, access computers or intercept communications) for the collection of security intelligence and, at the request of either the Minister for Defence or the Minister for Foreign Affairs, foreign intelligence, and

29 Irwin Cotler, Address to the Fifth Meeting of Ministers of Justice or of Ministers or Attorneys-General of the Americas, 28 April, 2004
30 Irwin Cotler, Evidence given to the Proceedings of the Special Senate Committee on the Anti-Terrorism Act, Ottawa, 21 February 2005

- The Minister for Defence is required to issue a ministerial authorisation before DSD can undertake activity to produce intelligence on an Australian person and, if the matter involves a threat to security, the Attorney-General must also agree.

Inspector-General of Intelligence and Security

The Inspector-General of Intelligence and Security is an independent statutory office holder appointed under the *Inspector-General of Intelligence and Security Act 1986* (Commonwealth). The functions of the Inspector-General are prescribed under sections 8, 9 and 9A of the Act.

The key role of the Inspector-General is to ensure that the intelligence agencies conduct their activities legally, behave with propriety, comply with any directions and guidelines from the responsible Minister and have regard for human rights, including privacy.

The Inspector-General:

- Conducts regular inspections and monitoring of agency activities
- Undertakes a formal inquiry into the activities of an Australian intelligence agency in response to a complaint or a reference from the Minister, and
- Can independently initiate own motion inquiries.

The Parliamentary Joint Committee on Intelligence and Security

The Parliamentary Joint Committee on Intelligence and Security is appointed under section 28 of the *Intelligence Services Act*.

Under section 29 of the *Intelligence Services Act*, the Committee's main functions include:

- To review the administration and expenditure of the AIC agencies, including their annual financial statements, and
- To review any matter in relation to any of the AIC agencies referred to the Committee by the responsible Minister or by a resolution of either House of the Parliament.

The Committee gives the Parliament an annual report on its activities during the year.

The courts

The Jack Thomas case illustrates the role of the courts in ensuring the legality of an agency's actions.

Jack Thomas was convicted in the Supreme Court of Victoria for offences which included intentionally receiving money from a terrorist organisation and falsifying a passport. The conviction was overturned by the Court of Appeal which ruled that a record of interview containing admissions was inadmissible. The interview had been conducted by a joint AFP-ASIO team in Pakistan. The decision indicates the procedures to be followed by Australian police officers conducting interviews in other countries if the records of those interviews are to be admissible in criminal proceedings in Australian courts[31].

31 (2006) VSCA 165

Officer training

Australian intelligence agencies take their legal and ethical responsibilities very seriously and train their staff accordingly.

The following examples illustrate ASIO and ASIS training in these areas:

- All decisions by ASIO officers are guided and informed by the ASIO Act, its Code of Conduct and its Values: Integrity, Excellence, Cooperation and Accountability. ASIO officers undertake mandatory training in 'Values, Ethics and Accountability in ASIO' in the induction program followed by refresher training every three years, and
- As part of the selection and training of its intelligence officers, ASIS looks for and imbues ethical behaviour in its staff. The commitment to ethical behaviour permeates all aspects of organisational culture from recruitment through training to deployment. Ethical conduct applies to the way ASIS officers manage their operations and the agents working for them.

The Inspector-General regularly reviews ASIO and ASIS files for both legality and the propriety of their operational conduct.

Independent National Security Legislation Monitor

The most recent addition to this supervisory regime is the Independent National Security Legislation Monitor.

The *Independent National Security Legislation Monitor Act 2010* (Commonwealth) provides for the appointment of an Independent National Security Legislation Monitor.

The appointment of the inaugural holder of this office was announced by the Acting Prime Minister, the Hon Wayne Swan MP, on 21 April 2011. In his media release, Mr Swan said:

> 'The Government introduced the legislation creating this new position in response to recommendations from the Parliamentary Joint Committee on Intelligence and Security, as well as recommendations from the Independent Security Legislation Review Committee (the Sheller Committee) and the Clarke Inquiry into the case of Dr Mohammed Haneef'.

The Monitor's functions are set out in section 6 of the Act. They are:

- To review, on his or her own initiative, the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation and any other law of the Commonwealth to the extent that it relates to Australia's counter-terrorism and national security legislation
- To consider, on his or her own initiative, whether any of that legislation contains appropriate safeguards for protecting the rights of individuals, remains proportionate to any threat of terrorism or threat to national security, or both and remains necessary
- If a matter relating to counter-terrorism or national security is referred to the Monitor by the Prime Minister – to report on the reference, and
- To assess whether Australia's counter-terrorism or national security legislation is being used for matters unrelated to terrorism and national security.

In summary, the Monitor will review the operation, effectiveness and implications of Australia's counter-terrorism and national security legislation, reporting to the Prime Minister and, through his or her annual report, to the Parliament.

The impetus for the legislation and this appointment can be found in the extensive parliamentary and public debates that surrounded the introduction of significant pieces of counter-terrorism legislation passed by the Parliament in the years following the terrorist attacks in the United States on 11 September, 2001.

However, there was no mechanism in the legislation, other than the usual process of parliamentary review, to monitor whether the balance between individual and community rights was still proportionate and being maintained over time.

In 2008, the Attorney-General, the Hon Robert McClelland, discussed the role of a similar position in the United Kingdom with the then British Independent Reviewer of Terrorism Legislation, Lord Carlile of Berriew QC.

The tradition of independent review of terrorism legislation in the United Kingdom stretches back to the 1970s. Between 1978 and 1984, reviews of the Prevention of Terrorism (Temporary Provisions) Acts and the Northern Ireland (Emergency Provisions) Acts were carried out by Lord Shackleton, Earl Jellicoe and Sir George Baker. Between 1984 and 2001 annual reports to the Parliament were produced by Viscount Colville and J J Rowe QC.

The brochure for a public lecture given by Lord Carlile at the Australian National University on 16 June 2009 states:

> 'He will argue that an independent person in this role can provide a level of public reassurance on the balance between regulation and civil liberties; and that he can proportionately influence debate and policy making. He will argue that national security is an important individual liberty in the context of current international terrorist activity.'

Lord Carlile held the position for more than nine years until he was replaced by David Anderson QC on 21 February 2011.

In welcoming the appointment of the Independent National Security Legislation Monitor, the Attorney-General, the Hon Robert McClelland said in his April 2011 newsletter:

> 'Keeping Australia safe is the job of security, intelligence and law enforcement agencies. The Government equips them with strong counter-terrorism laws to ensure they can do their jobs properly while ensuring there is necessary accountability and oversight. These laws were extensively reviewed during 2009 and 2010 and after a period of public consultation, were amended to ensure police have adequate powers to protect the community, especially in circumstances where a dangerous device or substance is involved.
>
> 'At the same time, additional protections that had been recommended by four different inquiries were included in the amending legislation, which passed through Parliament with the support of both major parties. This reflects a general consensus that the laws achieve the appropriate balance – this week's events (that is, the killing of Usama Bin Laden) have not created a situation where that balance needs to be recalibrated.

'Given the nature of these powers, the Government accepts the operation and effectiveness of the laws should be appropriately monitored.'

Need for regular monitoring

The national security laws regulating and conferring powers on the intelligence agencies and, in some cases, the Australian Federal Police require regular monitoring.

In reaching this conclusion, the Review has taken note of the safeguards and oversights contained in the present system as set out in this Appendix.

The Review considers the monitoring and review functions to be undertaken by the Independent National Security Legislation Monitor should provide significant reassurance to the government and the community that the strong powers granted under counter-terrorism and national security legislation will continue to contain appropriate safeguards and remain proportionate to the then existing threat of terrorism or threat to national security over the coming years.

The Independent National Security Legislation Monitor should be given time to establish himself in his role and to form his views on national security legislation before any significant amendments are considered which could affect the current balance of the legislation.

Staying ahead of the challenges to oversight and safeguards

The Review has considered the difficulties presented by issues that are running ahead of domestic and international legal frameworks or of significant sustained ethical analysis.

These issues include:

- The actions that can be taken against non-state actors: There are legal and ethical structures to deal with what can and cannot be done toward state actors engaged in hostile activity on the one hand and private citizens on the other. It is not clear that either framework is entirely suitable for dealing with non-state actors like terrorist organisations
- The use of Intelligence Surveillance and Reconnaissance platforms has been subject to criticism from human rights organisations. Close analysis of their concerns suggest that this is an area that requires considerably more deliberation. If the use of important new capabilities like these is to retain public support, there needs to be a clear articulation of any ethical issues involved in managing them effectively and the way they are used, and
- This Review is of the opinion that there needs to be international discussion and agreement about rules for and limits on cyber warfare.

A thoughtful exploration of these and other ethical issues in the right forums will make it far more likely that publicly acceptable boundaries can be determined by a constructive conversation rather than reactively by a defensive one.

It is important for the future operations of the AIC and intelligence organisations globally that the public understanding of these issues catches up with operational realities and possibly even gets ahead of them.

APPENDIX 4

METHODOLOGY

The Review conducted detailed investigations into the key issues raised by the Terms of Reference.

The Review invited and received thorough briefings and detailed submissions from the six intelligence agencies and several departments.

In addition, at the commencement of this Review, we called for public submissions in an advertisement published in:

- The *Australian Financial Review* on Friday 11 February 2011, and
- The *Australian*, the *Sydney Morning Herald*, the *Canberra Times* and the *Age* on Saturday 12 February 2011.

A list of submissions received by the Review is set out below in **Table 1**.

We conducted interviews with a wide range of interviewees including:

- The Prime Minister, Ministers, Shadow Ministers, Members of Parliament and former Ministers
- Heads of intelligence agencies, departmental Secretaries, heads of other Commonwealth organisations, senior military officers, think tanks and other commentators
- Heads or senior officials of counterpart intelligence agencies in the United States, Canada, the United Kingdom and New Zealand, and
- Officers engaged in operations in Afghanistan.

A list of organisations and people interviewed during the course of this Review is set out below at **Table 2**.

The Reviewers or members of the Review Secretariat conducted focus group sessions with middle ranking officers in each of the six intelligence agencies and some relevant departments. The focus groups are set out below in **Table 3**.

In all of its activities, the Review received full cooperation and assistance from the intelligence agencies, other interviewees and our international allies.

TABLE 1

SUBMISSIONS RECEIVED BY THE REVIEW

Attorney-General's Department

Australian Crime Commission

Australian Human Rights Commission

Australian Secret Intelligence Service

Australian Security Intelligence Organisation

Civil Liberties Australia

Comcare

Defence Imagery and Geospatial Organisation

Defence Intelligence Organisation

Defence Signals Directorate

Department of Finance and Deregulation

Department of Foreign Affairs and Trade

Department of Infrastructure and Transport

Department of Immigration and Citizenship

Department of the Prime Minister and Cabinet

Inter-Agency Security Forum (ASIO)

Leader of the Opposition

Media Gurus

National Archives of Australia

Office of National Assessments

Qantas

Returned and Services League

United Nations High Commissioner for Refugees

Mr Martin Brady AO

Mr Ian Dudgeon

Mr Maurice Horsburgh

The Hon John Howard AC

Mr Lance Joseph

Mr Frank Lewincamp PSM

Mr John McCawley

Mr Richard Morris

Mr Peter B Prosser

Mr Michael and Mrs Hylda Rolfe

Ms Rosemary Turner

Mr Faz Varjavandi

Professor Hugh White

TABLE 2

ORGANISATIONS AND PEOPLE INTERVIEWED BY THE REVIEW

Australian Government

The Hon Julia Gillard MP, Prime Minister

The Hon Kevin Rudd MP, Minister for Foreign Affairs

The Hon Stephen Smith MP, Minister for Defence

Senator the Hon Penny Wong, Minister for Finance and Deregulation

The Hon Robert McClelland MP, Attorney-General

The Hon Chris Bowen MP, Minister for Immigration and Citizenship

For the Hon Greg Combet AM, MP: Mr Allan Behm, Chief of Staff, Climate Change and Energy Efficiency

The Hon Brendan O'Connor MP, Minister for Justice and Home Affairs

The Hon Mark Dreyfus QC, MP, Cabinet Secretary

Members of Parliament

For the Hon Tony Abbott MP: Mr Mark Higgie, International Adviser to the Leader of the Opposition

The Hon Julie Bishop MP, Deputy Leader of the Opposition and Shadow Minister for Foreign Affairs

Senator the Hon David Johnston, Shadow Minister for Defence

The Hon Philip Ruddock MP, Shadow Cabinet Secretary

Former Members of Parliament

The Hon Peter Costello AC

The Hon Alexander Downer

The Hon Lindsay Tanner

Australian Public Service

Attorney-General's Department

Mr Roger Wilkins AO, Secretary

AusAID

Mr Peter Baxter, Director-General

Australian Crime Commission

Mr John Lawler APM, Chief Executive Officer

Australian Customs and Border Protection Service

Mr Michael Carmody AO, Chief Executive Officer

Mr Mike Pezzullo, Chief Operating Officer

Australian Federal Police

Mr Tony Negus APM, Commissioner

Mr Andrew Colvin APM, OAM, Deputy Commissioner Operations

Mr Peter Drennan APM, Deputy Commissioner National Security

Mr Michael Phelan APM, Deputy Commissioner Close Operations Support

Ms Rebecca Irwin, National Manager, Policy and Governance

Australian Transaction Reports and Analysis Centre

Mr John Schmidt, Chief Executive Officer

Australian Secret Intelligence Service

Mr Nick Warner AO, PSM, Director-General and staff

Australian Security Intelligence Organisation

Mr David Irvine AO, Director-General and staff

Department of Finance and Deregulation

Mr David Tune PSM, Secretary

Department of Broadband, Communication and the Digital Economy

Mr Peter Harris, Secretary

Department of Climate Change and Energy Efficiency

Ms Louise Hand, First Assistant Secretary, International Division

Department of Defence

Dr Ian Watt AO, then Secretary

Mr Stephen Merchant PSM, Deputy Secretary, Intelligence and Security

Mr Peter Jennings, Deputy Secretary, Strategy

Defence Imagery and Geospatial Organisation

Mr Steve Meekin AM, Director and staff

Defence Intelligence Organisation

Major General Richard Wilson AO, Director and staff

Defence Signals Directorate

Mr Ian McKenzie, Director and staff

Department of Foreign Affairs and Trade

Mr Dennis Richardson AO, Secretary

HE the Hon Kim Beazley AO, Ambassador to the United States of America

HE the Hon John Dauth AC, LVO, High Commissioner to the United Kingdom

HE Mr Justin Brown, Australian High Commissioner, Ottawa

HE Mr Paul O'Sullivan AO, High Commissioner to New Zealand

HE Mr Peter Varghese AO, High Commissioner to India

Mr Bill Paterson, Ambassador for Counter-Terrorism

Mr James Larsen, Ambassador for People Smuggling Issues

Dr Robert Floyd, Director-General, Australian Safeguards and Non-Proliferation Office

Department of Immigration and Citizenship

Mr Andrew Metcalfe, Secretary

Mr Lance Thomas, Director, Immigration Intelligence

Department of Infrastructure and Transport

Mr Mike Mrdak, Secretary

Mr Mick Palmer AO, APM, Inspector of Transport Security

Department of the Prime Minister and Cabinet

Mr Terry Moran AO, then Secretary

Mr Duncan Lewis AO, DSC, CSC, then National Security Adviser

Dr Margot McCarthy, then Deputy National Security Adviser

Ms Rachel Noble, then National Security Community Chief Information Officer

Mr Michael Shoebridge, then First Assistant Secretary, Defence, Intelligence and Research Coordination Division

Mr Peter Furlonger, Special Adviser, Defence, Intelligence and Research Coordination Division

Inspector-General of Intelligence and Security

Dr Vivienne Thom, Inspector-General of Intelligence and Security

Office of National Assessments

Mr Allan Gyngell AO, Director-General and staff

Office of the Australian Information Commissioner

Professor John McMillan AO, Australian Information Commissioner

Mr Timothy Pilgrim, Privacy Commissioner

Dr James Popple, Freedom of Information Commissioner

Parliamentary Joint Committee on Intelligence and Security

The Hon Anthony Byrne MP, Chair, and other Committee members

Prime Minister's Office

Mr Richard Maude, Senior Adviser – International, Defence, Trade

The Treasury

Dr Ken Henry AC, then Secretary

Australian Defence Force

Air Chief Marshal Angus Houston AC, AFC, then Chief of the Defence Force

Lieutenant General David Hurley AC, DSC, then Vice Chief of the Defence Force

Vice Admiral Russ Crane AO CSM, then Chief of Navy

Air Marshal Mark Binskin AO, then Chief of Air Force

Lieutenant General Mark Evans AO DSC, then Chief of Joint Operations

Air Marshal John Harvey AM, Chief Capability Development Group

Major General Gus Gilmore DSC, AM, Special Operations Commander Australia

National Security Committees

National Counter-Terrorism Committee

National Intelligence Coordination Committee

National Intelligence Collection Management Committee

Others

Professor Ross Babbage AM, Managing Director, Strategy International (ACT) Pty Ltd and Founder of The Kokoda Foundation

Dr Richard Brabin-Smith AO, former Deputy Secretary for Strategic Policy and Chief Defence Scientist

Mr Martin Brady AO, former Director, Defence Signals Directorate and former Chairman, Defence Intelligence Board

The Hon Catherine Branson QC, President, Australian Human Rights Commission

Mr Julian Burnside AO, QC, Victorian Bar

Mr Ian Carnell AM, former Inspector-General of Intelligence and Security

Mr Philip Flood AO, former Secretary, Department of Foreign Affairs and Trade, and head of the 2004 Inquiry into Australian Intelligence Agencies

Mr Michael L'Estrange AO, Director, National Security College, the Australian National University and former Secretary, Department of Foreign Affairs and Trade

Mr George Lekakis AO, former Chair, Victorian Multicultural Commission

Lieutenant General (Ret'd) Peter Leahy AC, former Chief of Army

Mr Frank Lewincamp PSM, former Director, Defence Intelligence Organisation

Dr James Renwick, Barrister, NSW Bar

Mr Richard Smith AO, PSM, former Secretary, Department of Defence

Dr Carl Ungerer, Program Director of the National Security Program, Australian Strategic Policy Unit

Professor Hugh White, Strategic and Defence Studies Centre, Australian National University

Overseas Partners

The United States of America

Central Intelligence Agency

Defense Intelligence Agency

Federal Bureau of Investigation

National Counterterrorism Center

National Geospatial-Intelligence Agency

National Intelligence Council

National Security Agency

Office of the Director of National Intelligence

President's Intelligence Advisory Board

US Department of State

US House of Representatives Permanent Select Committee on Intelligence

US Senate Select Committee on Intelligence

Ms Peggy Cloherty, Director, East Asia Group, Open Source Center

Dr Eliot Cohen, Johns Hopkins University

Dr David Gordon, Head of Research, Eurasia Group

General Michael Hayden, Chertoff Group

Dr Steve Kaplan, BoozAllenHamilton

Ms Ellen Laipson, President, Stimson Center

Mr John McLaughlin, Johns Hopkins University

Dr Jennifer Sims, Georgetown University

The United Kingdom

British Secret Intelligence Service

British Security Service, including the Joint Terrorism Analysis Centre

Cabinet Office

Government Communications Headquarters

UK Ministry of Defence

Mr Greg Shapland, Head of Foreign and Commonwealth Office Research Analysts Cadre

Lord Carlile of Berriew QC, former Independent Reviewer of Intelligence Legislation

Canada

Canadian Security Intelligence Service

Communications Security Establishment

Privy Council Office

Royal Canadian Mounted Police

Major General Christian Rousseau, Chief of Defence Intelligence

Mr William Baker, Deputy Minister for Public Safety

New Zealand

Department of the Prime Minister and Cabinet

Government Communications Security Bureau

New Zealand Security Intelligence Service

Rear Admiral Jack Steer, Vice Chief of the Defence Force

Colonel Angela Fitzsimmons, Director Defence Intelligence

Afghanistan

Major General Angus Campbell AM, Commander, Joint Task Force 633

Other officers and personnel who cannot be named for security and operational reasons

TABLE 3

FOCUS GROUPS

Australian Customs and Border Protection Service
Australian Defence Force
Australian Federal Police
Australian Secret Intelligence Service
Australian Security Intelligence Organisation
Defence Imagery and Geospatial Organisation
Defence Intelligence Organisation
Defence Signals Directorate
Department of Foreign Affairs and Trade
Department of Immigration and Citizenship
Office of National Assessments

ACKNOWLEDGEMENTS

The Reviewers express their appreciation to:

- The intelligence agencies and their officers for their complete and courteous cooperation throughout this Review
- The people and organisations who provided submissions or participated in interviews – their contributions and insights have been most helpful, and
- The members of the Review Secretariat for their professional, competent, conscientious and dedicated assistance.