STRATEGIC INSIGHTS

ASPI

121

The 2017 independent review of intelligence

Views from *The Strategist*

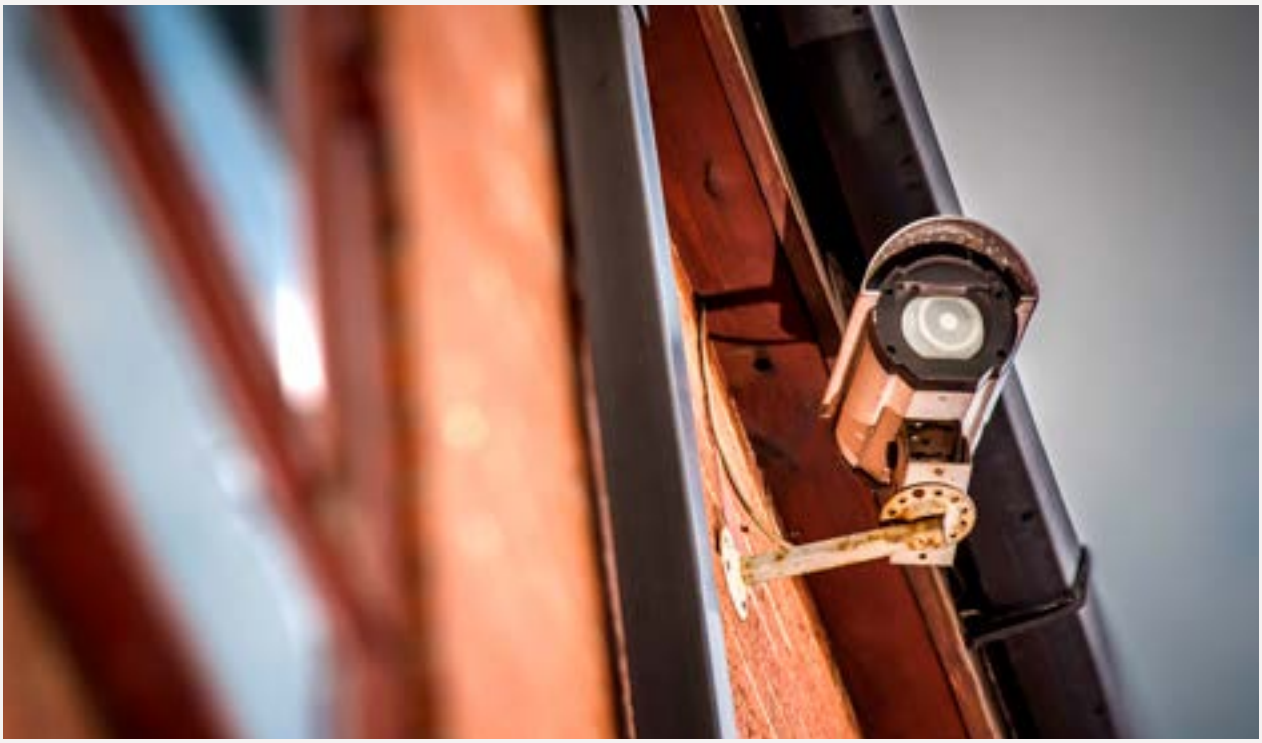
ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

James Clapper, Andrew Davies, Peter Edwards, Fergus Hanson, Peter Jennings

Introduction

Andrew Davies

Over the past 40 years, Australian governments have periodically commissioned reviews of the Australian intelligence community (AIC). The first such inquiry—the Hope Royal Commission of 1974—was commissioned by the Whitlam government as a way of shedding light on what had hitherto been a shadowy group of little-known and little-understood government agencies. It was also the beginning of a journey that would eventually bring the AIC more into public view and onto a firm legislative footing. The second Hope Royal Commission, in 1983, was partly a response to some dramatic external events, in the forms of the Coomb–Ivanov affair and a poorly judged Australian Secret Intelligence Service training exercise that went badly wrong. But it was also a continuation of the process begun by the previous commission.



External building security camera © CWS Managed Hosting/Flickr.

The structure of today's AIC and the oversight mechanisms under which it operates are products of those royal commissions. Strong oversight helps to regulate intelligence activities and manage the inevitable tension between secrecy and public confidence. The Hope reforms resulted in a layered and robust set of powers to protect the collective interests of the Australian polity. The scandals and political bickering that once accompanied some actions of intelligence agencies are largely things of the past. Since Justice Hope handed down his final report, no Australian government has seen the need for a third royal commission into intelligence.

But time doesn't stand still. Even as the Hope recommendations were being enacted, including the passing of some major pieces of intelligence-related legislation, the world around the AIC changed markedly. The Cold War came to an end, China rose from being an economic also-ran to the world's second-largest economy, and globalisation opened up the world in all sorts of positive ways, but with the downside of also enabling sophisticated transnational crime and terrorism.

Not surprisingly, from time to time in the intervening period Australian governments have seen the need to test the assumptions underpinning the nation's intelligence arrangements. The first such review—a sort of post-Hope health check—took place in the early 1990s. There was another in 2004, driven by the prominent role that intelligence—subsequently shown to be wrong—played in the decision to go to war in Iraq in 2003. The Gillard government also commissioned an intelligence review in 2011, motivated simply by best practice.

Each of those reviews adjusted the way in which the AIC interacts with the government and the public. There were some worthwhile reforms, but no 'headline' changes. In fact, a bigger change in that period was the passing of the Intelligence Services Act in 2001, which is probably fairly described as the last brick in the Hope architecture.

The most recent review, and the one that concerns us here, is probably more 'activist' in its recommendations than any other post-Hope review. Reviewers Michael L'Estrange and Stephen Merchant, and adviser Sir Iain Lobban, have a wealth of hands-on experience of intelligence management. They applied that experience to the challenges faced by today's intelligence agencies as they grapple with a range of complex problems, from nuclear proliferation and state-on-state espionage to international criminal and terrorist organisations.

As you'll read in the articles that follow, changes recommended by the review would change the profile of intelligence within the government, giving it a much more prominent place in the Canberra pantheon. And they would more tightly integrate the intelligence functions that reside in government departments outside of the 'traditional' agencies (including those in the Australian Federal Police and the Department of Immigration and Border Protection) with the rest of the AIC. The oversight mechanisms of the AIC would also get a shakeup, with the remit of the Parliamentary Joint Committee on Intelligence and Security being widened, and the Inspector-General of Intelligence and Security being allocated significantly greater resources.

The articles reprinted here give a range of perspectives on the review and its recommendations. They originally appeared on ASPI's commentary and analysis website, *The Strategist*, where you can always find a lively discussion of the policy issues of the day.

The 2017 review of intelligence: a first look

Andrew Davies, 19 July 2017

There's an air of 'continuity with change' about the new Independent Intelligence Review. The review almost flew under the radar this week amid all of the other changes to Australia's national security apparatus. This post is my initial reflection on the review's main recommendations.

As for continuity, it's clear that the reviewers, Michael L'Estrange and Stephen Merchant, found most of the existing arrangements to be fit for purpose: 'The clear dividing lines [that Justice Hope's royal commissions of the 1970s and '80s] highlighted—between

foreign and security intelligence, intelligence and law enforcement, intelligence collection and assessment, and intelligence assessment and policy formulation—continue to provide the foundations of Australia's intelligence community. We assess those delineations have broad enduring relevance.'

Following that assessment, it's perhaps a little surprising that one of the major recommended changes was the establishment of a new Office of National Intelligence, to be located in the prime minister's portfolio. While that would bring Australia's intelligence arrangements into line with the other Five Eyes partners (Canada, New Zealand, the UK and the US), the need for the new office isn't immediately clear. Under the existing arrangements there's already a statutory responsibility on the Office of National Assessments to play a coordination role. Section 5 of the ONA Act says that one of the functions of the office is 'to coordinate the foreign intelligence activities that Australia engages in, including in relation to setting Australia's foreign intelligence requirements based on Australia's foreign intelligence priorities'.

So the coordination mechanism is already in place, at least as far as foreign intelligence activities are concerned, and it has been running smoothly for many years. But the review observes that the contemporary threat environment is increasingly transnational in nature, and that there's more overlap between foreign and domestic intelligence requirements than hitherto, especially in the area of counterterrorism. The argument for the new ONI to have a wider remit than ONA (which it will subsume) seems to come down to a tighter integration of foreign and domestic security intelligence.

I'm not entirely convinced by that argument, for two reasons. First, as ASIO will tell anyone within earshot, it is emphatically *not* a 'domestic spy agency'. Its work has had an international aspect for as long as the agency has existed, and it seems to have managed perfectly well. Second, the multi-disciplinary National Threat Assessment Centre was stood up in 2003, and has been a demonstrable success in coordinating domestic and foreign intelligence activities and law enforcement. The centre's work has been behind many of the successful disruptions of planned terrorist acts.

The other thing that puzzled me on my first reading was the recommended change of status of the Australian Signals Directorate, the national signals intelligence and information security agency. ASD has long resided in the Department of Defence for management purposes, as befits its important role in supporting military operations. But it has also had another hat as a national agency and information security authority. The review recommends putting the emphasis more on the 'national' role and making ASD a statutory body, though (confusingly) it will remain in the Defence portfolio. But ASD will no longer be subject to the 'efficiency dividends' (an Orwellian term for budget cuts) that other agencies in the portfolio have to absorb.

Freeing ASD from the efficiency dividend is a worthwhile step. The demand for its services has increased sharply in recent years, mostly because of the increasing importance of its defensive and offensive cyber activities, as well as its terrorism-related work. From discussions, it's clear that ASD has suffered badly from the dual pressures of less money—and hence fewer staff—and more demand. It has also suffered when trying to recruit IT-savvy personnel for its cyber arm, and four years of zero wage growth made an already difficult situation worse. But surely the government could simply have instructed the previous Defence secretary to allocate ASD an appropriate budget? It's hard to avoid the conclusion that this is another piece of evidence that Russell Hill has largely been an ungoverned fiefdom in recent years.

In any case, there'll need to be a substantial rewrite of the corresponding legislative framework. Since 2001, the activities of ASD and the two other foreign intelligence collection agencies (the Australian Secret Intelligence Service and the Australian Geospatial-Intelligence Organisation) have been regulated by the Intelligence Services Act. With ASD becoming a statutory body, it will presumably require its own Act, which might be a good thing in some ways. While ASD's signals intelligence function plays the same broad security role as the human and geospatial intelligence activities of ASIS and AGO, respectively, its cyber activities are distinctly different. A tailored legal framework will be helpful as cyber operations mature. An alternative approach might have been to split off signals intelligence from cyber, but that also has pros and cons—which the US has been grappling with.

On balance then—and I stress that this is based on my first reading of the report—the major changes that have been announced don't seem to be aimed at solving obvious problems. (That could also be said of all of this week's announcements.) But they also result in new arrangements that, if carefully implemented, could build on existing strengths. Hopefully the working parts of the existing model will undergo minimalist changes.

One thing I haven't mentioned in this post is the oversight of intelligence. I'll come back to that next week.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/2017-review-intelligence-first-look/

The good and not so good of policymaking

Peter Jennings, 21 July 2017

The most important point to make about the government's proposed Home Affairs portfolio is that these new arrangements can be made to work. They will not harm our counterterrorism performance and could improve Australia's underwhelming efforts to protect against foreign interference and strengthen the security of critical infrastructure. But in announcing last Tuesday what Prime Minister Turnbull called 'the most significant reform of Australia's national intelligence and domestic security arrangements—and their oversight—in more than forty years', it's surprising that so little groundwork had been done to justify the need for change or to say how it was going to be done.

The Home Affairs announcement was linked to the government's release of the unclassified version of the 2017 Independent Intelligence Review. By contrast, this is a meticulously argued report based on extensive consultations and containing detailed recommendations and implementation strategies that will significantly reshape the Australian intelligence community. The prime minister said that the government would accept some of the review's key proposals and that a 'task force' in the Department of the Prime Minister and Cabinet could consider other recommendations 'in detail.' Changing tack, Mr Turnbull then said, 'In these difficult times, repeated reviews and task forces are not enough. We need to take more decisive action.' With that the Home Office was announced, with promises that detailed implementation arrangements would be worked out in the second half of this year and 'its roll-out to be complete by 30 June next year'. There is indeed more than one way to skin a policy cat.

The fallow period of implementation planning creates a policy mammoth moving slowly across the tundra of Australian politics. Will the beast still be alive in June 2018? Government should move quickly to shape the policy debate by issuing a discussion paper that sets out, as clearly as possible, the strategic reasons for making these big changes and addresses some of the questions that have arisen in the last few days. For example, how will ASIO and the AFP 'retain their current statutory independence, which is such a vital aspect of the Australian system', as the PM said, while the Home Affairs portfolio 'oversee[s] policy and strategic planning and *the coordination of the operational response* to the threats we face' at the same time? [My emphasis.]

More clarity is needed around the handling of ministerial warrants and authorisations for ASIO and AFP activities. The PM said that the Attorney-General 'will retain his current role in the issue of warrants and ministerial authorisations'. But he also said that the government will 'review the role of the Attorney-General in the role in ASIO's operations in the work to design and establish the new portfolio to ensure continued and efficient oversight'. When pressed about whether ASIO and AFP warrants and authorisations would require the signature of one or two ministers, the Attorney-General seemed to suggest that both he and the Home Affairs minister would authorise actions, saying that for certain types of ASIS and ASD actions 'there are two hands, as it were, on the mechanism to ensure that a warrant or an authorisation has the oversight and scrutiny of two ministers and not one'. So, the Attorney-General will be either the sole approver of warrants, or one of two ministers. But on the third hand, the Attorney-General may not have any oversight role after yet another review. Clear?

The recommendations in the intelligence review are certainly clear and well thought through. The current Office of National Assessments undergoes a subtle but important name change to the Office of National Intelligence—the significance being that the

ONI will take on a stronger leadership role of the intelligence community, not simply be the drafter of community-wide national assessment reports. The agency's director-general position will be elevated to the level of a departmental secretary and will be more analogous to the US Director of National Intelligence in function. The DG-ONI will become a centrally important figure in discussions at the National Security Committee of Cabinet. The ONI is recommended to have a 50% increase in analytical staff, addressing a systemic weakness in the intelligence community, which can often be one-person deep in terms of real expertise on specific countries and issues.

The government has accepted the review's recommendation to make the Australian Signals Directorate a statutory authority within the Defence portfolio. This continues ASD's journey to becoming something more like the UK's GCHQ, which is separate from but works closely with defence. This is the end of a turf battle in which Defence lost a major crown jewel. How did that happen, chaps?

There's a lot more to the L'Estrange–Merchant review, including sensible measures to strengthen the ministerial warrants system over certain types of intelligence operations and to boost the role of the Parliamentary Joint Committee on Intelligence and Security, which has done sterling work in the last few years and is one of best committee appointments for aspiring backbenchers. It's a pity the government didn't clearly commit to implementing all of it, instead of cherrypicking some recommendations and passing the rest to a PM&C 'task force' to consider. Why do reviews like this if the final product is then opened to public service predation? It's not as if the government didn't have the chance to react to drafts as the study developed.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/good-not-good-policymaking/

Design for a secure home

Peter Jennings, 22 July 2017

In a week dominated by the government's announcement to establish a home affairs portfolio, the release of the 2017 Independent Intelligence Review report got less attention than it deserved. That's a pity because the review is a rare thing in the policy world now. It's carefully researched, makes sensible recommendations and will strengthen the performance of Australia's already capable intelligence community.

The key reviewers were Michael L'Estrange, a former secretary of the Department of Foreign Affairs and Trade and international adviser to John Howard; and Stephen Merchant, who has headed the Australian Signals Directorate and was a deputy secretary in Defence with deep experience of the intelligence world.

Neither man is in the business of political gamesmanship or interested in Canberra's public service rituals of fighting for bureaucratic power. Their review is as straight an assessment as one can get about how the intelligence system needs to be reshaped to handle a risky strategic environment that, the authors judge, is quickly deteriorating.

L'Estrange and Merchant argue that a rising competition for influence between states, the spread of missiles and more lethal military technology, the growth of extremism and terrorism, and the interdependence of countries through information technology and economic links combine to make the world less predictable and threats more immediate.

They see a worrying trend of international and domestic security risks becoming more interconnected. Our intelligence system was designed around keeping foreign and domestic security arrangements separate. Now the challenge is to make our 10 intelligence agencies operate more like a single enterprise.

With considerable understatement, the report says:

> 'Assumptions that have long underpinned Australia's security and foreign policy, including those in relation to the strength of the rules-based component of the global order, will be more uncertain.'

That's a subtle hit against the government's 2016 defence white paper, which used the phrase 'rules-based global order' no fewer than 42 times. But just wishing to keep something that is fast disappearing won't protect Australia's interests. To boost our security, L'Estrange and Merchant argue for 'at least a 50 per cent increase in current analyst numbers' in Australia's peak intelligence agency, the Office of National Assessments.

The government has accepted the recommendation that the ONA will undergo a small but important name change to the Office of National Intelligence, to be headed by a secretary-level director-general reporting to the Prime Minister. ONI will take on a much broader role and have the financial clout to set intelligence collection and analysis priorities for the whole intelligence community. With money comes power, and the DG ONI will control future intelligence investment and advise government on who to put into senior intelligence jobs.

The most important change is the proposed relationship with the Prime Minister. L'Estrange and Merchant recommend that the director-general signs off on a daily morning intelligence brief for the Prime Minister. A daily intelligence briefing copies the US President's morning brief. The US intelligence community went into panic stations when Donald Trump declared he didn't want such a product. Even with Trump's peculiarities, it's still true that the combination of knowledge and access to the President is a powerful asset for intelligence agencies.

The daily theatre of the Prime Minister receiving a morning intelligence briefing will transform the DG ONI into one of Canberra's most influential security officials, and the change will strengthen the Prime Minister's ability to steer his national security committee of cabinet.

A second subtly important change recommended by the review, and agreed by government, is to move the Australian Signals Directorate from under the control of the Defence organisation.

ASD has been taking on an increasingly central national role because of the all-pervasive influence of cyber technology in business and daily life. But the agency is also a critical part of the way the Australian Defence Force fights in current and future operations.

Defence would have resisted losing such a gem. Consider this characteristically understated line in the intelligence review:

> 'For ASD, the option of continuing to operate within the Department of Defence's employment framework … is not the most effective way forward. It would increase the risk of losing additional critical talent, skills and capabilities. ASD needs to be more in control of its own destiny.'

Defence, in other words, was mismanaging ASD to such a degree that the only way to fix the problem was to remove it from the control of the department. If that's not worth a parliamentary inquiry, then what is? ASD will be autonomous, although it will still report to the Minister for Defence.

It has been correctly reported that the review did not comment on the merits of creating a home affairs portfolio but L'Estrange and Merchant made some observations that should be carefully considered by Peter Dutton, the minister-designate for home affairs. It's vital that intelligence assessments are made independent from policymaking influence.

Intelligence assessments must speak truth to power. L'Estrange and Merchant say:

> 'If the content of intelligence assessments is influenced by preordained policy priorities and preferences, those assessments lose their credibility.'

This recalls the allegations of No 10 'sexing up' Britain's Iraq weapons of mass destruction intelligence dossier in 2003. More directly, the proposed home affairs portfolio will bring together several intelligence collection and analysis agencies and hard-edged policy implementers in Border Force, the Australian Federal Police and the Department of Immigration (which itself has a large intelligence arm).

It's quite possible to design the home affairs portfolio in ways that will address the separation of roles and responsibilities of intelligence and policy agencies, but this week Malcolm Turnbull said the super-department would pool some critical functions. It 'will oversee policy and strategic planning and the co-ordination of the operational response to the threats we face'. Implementing the home affairs construct will require careful design and separations between its component entities.

One potential problem area untouched by the review is that the two remaining intelligence organisations in Defence—the Defence Intelligence Organisation and the Australian Geospatial-Intelligence Organisation—report to a deputy secretary who is also responsible for strategic policy development within Defence. That was the result of an earlier review that identified 'improved career development' as one reason to bring policy and intelligence functions under one deputy secretary. With the Iraq 'secret dossier' precedent firmly in mind, that's one Defence initiative that should be quickly reversed.

There is much to commend the intelligence review but government should realise that the recommendations will not be implemented cheaply. The cost of Australia's intelligence community is already nearing $2 billion annually, but such is the worrying state of our strategic outlook that figure will continue to grow.

An early, indeed urgent, target for more intelligence analysis must surely be North Korea. Our endless calls for North Korea to bend to the 'rules-based global order' are falling on deaf ears in Pyongyang.

Government should ask the intelligence community to start applying the L'Estrange and Merchant principles for 'enterprise-level management' in a special intelligence taskforce on North Korea. Our allies could only benefit from an Australian perspective. Regrettably, we may have cause to draw on that intelligence product sooner than many people think.

For print readers, the original piece with live links is at https://www.aspi.org.au/opinion/intelligence-review-design-secure-home

The intelligence review: the cybersecurity dimensions

Fergus Hanson, 25 July 2017

The cybersecurity dimensions of the 2017 intelligence review report have been mostly overlooked, but it contains some interesting recommendations, as well as leaving considerable detail still to be worked out. The proposals don't fix all the issues faced by a system coming under heavy strain, but they add potentially helpful adjustments, several of them aligned with ASPI recommendations.

The big changes centre on the Australian Signals Directorate (ASD) and the Australian Cyber Security Centre (ACSC). The ACSC will formally operate as part of the ASD, with one minister having primary responsibility for the ACSC and cybersecurity. That minister is likely to be the new super-duper minister, Peter Dutton, but that's still to be determined.

The new head of the ACSC will be the prime minister's special adviser on cyber security, Alastair MacGibbon, who will serve 'as the single focus of accountability to the Government for cyber security'. The review proposes merging his team in PM&C into the ASCS. While that move makes a lot of sense, it could create some potentially challenging ministerial reporting lines that the taskforce set up to implement the changes will need to resolve. For example, depending on who the head of the ACSC ultimately reports to, MacGibbon could be reporting to the Home Affairs minister with his ACSC hat on, to the PM with his special adviser hat on, and to the Defence minister with his ASD hat on (given that the ACSC sits under ASD). The big advantage of the move is that putting MacGibbon in charge of the ACSC joins up his policy role with the doing side of the equation.

Centralising cybersecurity policymaking and drawing the operational agencies into one centre should improve MacGibbon's ability to encourage government departments to step up their cybersecurity defences. To facilitate that, the review suggests supporting more secondments from across government into the ACSC and allowing staff 'to retain their existing organisational authorities and ability to access data, information and capabilities from their home organisations'.

At present, MacGibbon faces what must be a very frustrating ritual of being hauled before Senate Estimates and asked to explain why government departments keep failing to meet minimum cybersecurity standards, while simultaneously having no authority to force them to step up their game. This change doesn't fix that disconnect, but it's a move in the right direction by combining policymaking with operational agencies.

With MacGibbon's strong links to industry, the new arrangement should also help improve industry engagement, including within the Joint Cyber Security Centres, which the review proposes remain the responsibility of the government's computer emergency response team, CERT Australia (which is also likely to move from the Attorney-General's portfolio to Home Affairs and be placed within the ACSC).

The suggested appointment of an intelligence coordinator for cybersecurity 'to meet and manage the growing expectations of the ACSC, particularly in safeguarding the security of government networks' also makes sense. That official would report to the head of the ACSC.

The suggestion to stand up a 24/7 'capability to manage public messaging and policy advice in relation to rapidly emerging cyber events' is a strong one, given Australia's thus far advantageous time zone, which gives us a handy lead time to prepare for attacks that are first unleashed on the other side of the planet. It should also assist with communication deficiencies highlighted by recent cyber incidents.

The move to officially broaden ASD's mandate is another important change, and updates its role to fit contemporary realities. As my colleague Andrew Davies has noted with encryption, there are plenty of areas where our legislation is lagging.

Finally, the review provides some striking assessments of the cyber-threat landscape, suggesting this is a beginning rather than the end:

> One of the most worrying aspects of technological change is the way it is helping to place enormously destructive capabilities within easier reach of rogue states and non-state actors. This trend is not reversible and it will lead to an even more threatening international environment than now exists.
>
> In our view, the challenge of protecting the integrity, confidentiality and availability of systems and data will only become more important and more complex. Defensive and proactive technical security measures will increasingly be at the core of strategies to secure systems and data. Whether it is in relation to data analytics, encryption, decryption, data protection generally or the use of cyberspace, collaboration and co-operation between Australia's intelligence agencies and the private sector will become increasingly necessary and relevant, not least because in important specific areas private sector ICT innovation and technology application are more advanced.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/intelligence-review-cybersecurity-dimensions/

The intelligence review: our Hope for years to come

Peter Edwards, 26 July 2017

Peter Jennings accurately described the contrast between two examples of structural policymaking last week, the announcement of the new Home Affairs portfolio and the release of the unclassified version of the 2017 Independent Intelligence Review. Jennings was also right to argue that discussion and implementation of the review should not be submerged beneath the tumult over the incorporation of responsibility for ASIO and the AFP, along with immigration and border protection, under the Home Affairs umbrella.

Much of the review's value arises from the authors' deep knowledge of the history of reform of the Australian intelligence agencies. Michael L'Estrange and Stephen Merchant place their analysis and recommendations into the context of the two royal commissions conducted by Justice Robert Hope in the 1970s and 1980s, which gave the Australian intelligence community the shape it has had for the past 40 years. They are well equipped to do so. L'Estrange was a researcher for the second Hope royal commission and was greatly impressed by Hope's intellectual and personal qualities. He has held a number of posts, including secretary of DFAT and Cabinet secretary, which have enabled him to observe the agencies at close quarters. Merchant has held a number of senior posts in several of the agencies shaped by Hope. They are two experienced insiders, building on the work of a remarkably effective outsider.

L'Estrange and Merchant take as their baseline the Hope royal commissions' definitions of the roles and responsibilities of the intelligence agencies, the oversight and accountability mechanisms under which they should operate, and the operational principles they should observe. After examining the current security environment, they express their recommendations as extensions, amendments or revisions of the structures and principles developed by Hope.

The central concern of Hope's 16 major reports—striking the right balance between national security and civil liberties—remains fundamental, but L'Estrange and Merchant argue that some of the other crucial distinctions he made—'between intelligence collection and assessment, between human intelligence and signals intelligence, between intelligence assessments and policy determination, and between security intelligence and law enforcement' (paragraph 2.17)—can no longer be applied as rigidly as Hope did. By being so frank, they provide an intellectually robust framework within which to discuss their recommendations.

The review's two most important recommendations are logical and timely extensions of Hope's work. The first is the expansion of the Office of National Assessments (ONA) into the Office of National Intelligence (ONI). The creation of ONA was probably Hope's single greatest innovation. He saw the need for greater coordination between agencies that had too often been divided by geographical distance and institutional rivalries. Hope envisioned a central agency, devoted solely to assessment—unlike the US Central Intelligence Agency, which combines assessment, collection and special operations. By no coincidence, ONA's new headquarters in 2011 was named the Robert Marsden Hope Building.

The review tackles, firmly but tactfully, the false expectations that some have entertained over ONA's role and sets out clear reasons why it should be developed into an ONI, along the lines of the coordinating bodies in Australia's Five Eyes partners.

Turning ONA into ONI has potential risks as well as likely benefits. L'Estrange and Merchant emphasise the importance of preserving the independence of intelligence assessments, while also saying that assessments must be timely and relevant to policymakers. Both statements are right, but getting the balance between relevance and independence will be no easy matter. Similarly, there is potential tension between two stated aims, greater coordination and greater contestability. How can we ensure that assessments are contested, without descending into interagency rivalry (like the notorious FBI–CIA antagonism before 9/11), and that the agencies are coordinated, without succumbing to groupthink? There are no simple answers, and outcomes depend on personalities and organisational cultures as much as on structures. The review's recommendations seem wise, if implemented with the designated checks and balances. The ONA can rightly be housed in the Robert Marsden Hope Building.

The review's second major recommendation is that the Australian Signals Directorate (ASD) be turned into a statutory authority with increased responsibilities and resources. This, too, is an extension of Hope's arguments. Hope was ahead of his time in foreseeing an important future for signals intelligence, then handled by a division in the Department of Defence. He urged that it be given greater autonomy from the defence minister and secretary. Today, when everyone recognises the importance of cyber as an arena of international contest, turning ASD into a more influential and independent agency is a logical further step in the direction initiated by Hope.

The office of the inspector-general of intelligence and security emerged from Hope's second royal commission. The intelligence review rightly insists that, as the agencies increase their roles, responsibilities and resources, so should the accountability and oversight bodies. The review's recommended augmentation of the office is entirely consistent. Hope, however, doubted whether a parliamentary committee was appropriate in the Australian system. The Hawke government decided on a very limited model, which has had its remit extended over the years. The review's proposal for further extension of the committee's role is consistent with the views of (PDF) the respected former Labor senator and minister for defence, John Faulkner.

There is much else in the review that should form the basis of calm and rational discussion and prompt implementation. Any discussion should start from the basis that this review is the most thorough, comprehensive and clearly argued assessment of the intelligence agencies since the Hope royal commissions; that it consciously aims to bring the structures and principles enunciated by Hope into the current strategic environment; that it is frank about the areas in which those structures and principles require revision; and that constructive discussion and prompt implementation should not be submerged beneath the controversy over the establishment of a Home Affairs portfolio.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/intelligence-review-hope-years-come/

Australia's intelligence reforms: lessons from the United States

James Clapper, 28 July 2017

During my recent engagement with the Australian National University's National Security College, I was asked whether Australia would benefit from having a Director of National Intelligence, similar to the position I held in the United States from 2010 until January this year.

Knowing that a review of Australia's intelligence arrangements was then wrapping up, I was a little reticent to offer gratuitous advice. Now that the Review is out there, and Prime Minister Turnbull has announced his intention to establish an Office of National Intelligence, I thought I would outline my views in a little more detail.

First, I commend Australia for its practice of conducting regular reviews of the effectiveness of its intelligence community and recommending improvements. We in the United States do not do that—our reviews are more sporadic and anecdotal. The last time we made any major change to our intelligence community, it was in response to a traumatic event—the 9/11 terrorist attacks. In comparison, changes Australia makes have not commonly been impelled by extreme circumstances.

Second, if Australia made no changes to its intelligence posture, it would still have a very competent, professional intelligence community. I have worked with the Australian intelligence community for over 30 years in many capacities, and I can attest to its maturation, sophistication, and tremendous capabilities of Australian intelligence. In the intelligence space, the United States does things with Australia that we do not do with any other ally.

Third, while there are many very thoughtful recommendations in the 2017 Review, the one I would (not surprisingly) like to focus on is the analogue to the US Director of National Intelligence.

An Australian version of this position, tailored for local circumstance, makes great sense, for essentially the same reason it makes sense in the US context. I found great strength in the integration of US capabilities across our 17 components, all but two of which reside in one of six cabinet departments.

There are many common denominators across the functions of intelligence, and many enterprise similarities. This stems from the simple but profound truism that the sum is greater than its parts—US experience shows that when the complementary capabilities of our various intelligence components are synthesized and melded, we end up with more complete intelligence products and services for our decision-makers. This applies whether that decision maker resides in the Oval Office, or, to stretch the metaphor, an oval foxhole.

Yet integration and coordination across organisational boundaries will not happen by itself. It requires a full-time champion and advocate with both internal and external constituencies.

One of the most important forms of leverage to encourage this integration is through the allocation of resources. Where is the manpower and money allocated, across the enterprise? Where should we make investments, and where should we make divestments? Moreover, I can attest, this works much better if this is done with a strategic overview, rather than on a stovepipe by stovepipe—Australians might say 'silo by silo'—basis.

Hopefully, the director general of the Australian Office of National Intelligence will have this perspective and the authority to do something with it. It was critical to me in the US system.

Who the first DG ONI is will be hugely important because of the precedents that he or she will set for successors. If I were king, which I clearly am not, I would recommend someone steeped in intelligence, preferably having served as an agency director—knowing all the players will be key to championing integration, collaboration, coordination on a day-to-day and systematic basis.

It is worth emphasising that style counts. Furthering integration, coordination and collaboration across the Australian intelligence community will require artful persuasion and integrity, not overbearing force.

Back in 2010, just before nominating me as DNI, President Obama invited members of my family to the Oval Office. The President said to my granddaughter 'I really appreciate your grandfather taking on the *second* most thankless job in this town.'

The inaugural head of the Office of National Intelligence will have thankless days ahead of them, but this is a smart reform, and we should all wish them well.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/australias-intelligence-reforms-lessons-united-states/

The 2017 review of intelligence: the legislative angle

Andrew Davies, 5 August 2017

In my previous post on the recently released 2017 Independent Intelligence Review, I promised to come back to the subject of oversight. But before we get to that, it's important to understand the legislative framework under which oversight will take place. (Thus this series of posts now becomes a trilogy.)

As I noted earlier, implementing the organisational changes recommended by the review will entail making a number of legislative changes. In particular, the Office of National Intelligence will require a new legislative instrument in order to subsume the Office of National Assessments, which currently operates under the ONA Act. And putting the Australian Signals Directorate on a statutory footing will require—at least—a modification to the Intelligence Services Act.

But the review has much more to say about the legislative basis for the activities of the Australian intelligence community (AIC). In particular, there's an entire long and thoughtful chapter devoted to the subject. I'll try to summarise what I see as the most important points, as well as discussing some questions that it raised in my mind, but I'd encourage interested readers to take the time to read chapters 6 and 7 of the review in full.

Chapter 6 of the review begins with a survey of the existing raft of legislative instruments. It observes that the current framework has evolved over time, and that the net result is a less than cohesive combination of enduring principles and ad hoc provisions that cater for changes in the composition of the AIC and the external threat environment. The authors ultimately recommend an end-to-end review of the legislative basis for the AIC:

> We recommend a comprehensive review of the Acts governing Australia's intelligence community be undertaken to ensure agencies operate under a legislative framework which is clear, coherent and contains consistent protections for Australians.

That's a sensible recommendation, and it's something that should probably happen every 20 years or so. There are enduring principles that should always be reflected in a democracy's intelligence-related legislation, but technological and societal changes can render the specifics of even well-crafted legislation unworkable over time. The difficulties of dealing with modern encryption technologies under an interception framework based on the 1970s-vintage Telecommunications Interception Act are a case in point in *The Strategist* posts *Going dark—strong encryption and security (part 1)* and *Not dark yet—strong encryption and security (part 2)*.

A review of nine major pieces of interrelated legislation won't be something that happens on a timescale of weeks or even months. So the review also makes some recommendations about changes that could be made to existing laws to streamline processes and remove unnecessary (and often unanticipated) impediments to AIC activities. Most of the recommendations are sensible and unremarkable. For example, when two AIC agencies are cooperating on an activity, the review recommends that they be authorised to raise a joint request for a ministerial authorisation, rather than one each, as is currently the case—even when the requests go to the same minister (paragraph 6.60).

Less uncontroversial are some of the proposals for changes to the ability of AIC agencies to collect intelligence related to Australians. That is the essential tension in the practice of intelligence in a democracy, and so any proposals for change require rigorous justification, and the public is owed a clear explanation. That said, I don't think too many people would object to the notion of 'inferred consent' (paragraph 6.46) of Australians *in extremis.* For example, I think most of us would want Australian authorities to act without delay if we were kidnapped by pirates or a terrorist group. The proposed change would allow the AIC to get to work immediately, without going through an authorisation process.

I'm less convinced of the review's argument that no authorisation should be needed retrospectively in cases of inferred consent. After all, the case ought to be a slam dunk, and I don't think there's any reason not to keep the bar high for protecting Australians' rights.

In fact, the review shows a commendable respect for existing protections of Australians. For example, it considers the proposition that the degree of intrusiveness of AIC activity on individuals could form the basis for deciding whether a ministerial authorisation is needed. The authors rightly conclude that it should not (paragraph 6.39):

> Using intrusiveness as a defining principle could basically limit [Ministerial authorisations] to activities overseas that would require a warrant if conducted in Australia. This would mean most of ASIS's current activities to produce intelligence against an Australian would not need an authorisation at the Ministerial level. We are of the view that this approach would diminish the rights of Australian persons in an unacceptable way.

One point on which I'm not entirely convinced (at least based on the detail provided in the unclassified review report) is the section titled 'Class Authorisations – Australians Involved with Terrorist Groups' (paragraphs 6.30–6.35). The proposed change concerns Australians 'whose involvement with terrorist organisations proscribed by the Attorney-General under the Criminal Code constitutes a threat to national security'. So far, so good, but what does 'involvement with' mean? That's important, because we are told that class authorisations are needed because they 'would allow the [Intelligence Services Act] agencies to respond quickly to developing threats from previously unidentified individuals, a more common occurrence now with the emergence of 'lone wolf' attackers'.

But 'lone wolf' attackers have only loose affiliations with terrorist groups, almost by definition. To sign up to such a proposal, I'd want to know where the threshold for involvement is set—does someone have to self-identify as a member of ISIS, for example, or

would visiting an ISIS website be enough for inclusion in the class? What if someone posts online supports for the religio-political ideal of a caliphate, but gives no indication of crossing the line into violent activity?

All changes to intelligence-related legislation inevitably involve balancing freedoms and security. The devil is always in the detail, and the review's recommendations are yet to be translated into draft laws. Regardless of whether the proposed major review takes place, the Independent National Security Legislation Monitor is going to have a lot of work to do!

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/2017-review-intelligence-legislative-angle/

The 2017 review of intelligence: keeping watch

Andrew Davies, 29 August 2017

In previous posts I looked at the major structural reforms recommended in the recent intelligence review and at the legislative changes that will be required to implement them. Today I look at the oversight of the Australian intelligence community. As usual, I'll recommend that readers refer to the review for more detail (chapter 7 pertains).

Australia's robust oversight mechanisms owe their existence to the two Hope Royal Commissions on intelligence and security in 1974 and 1983. As Peter Edwards pointed out in *The Strategist* recently, Hope really knew his stuff, and the layered ministerial, legislative, parliamentary and statutory oversight mechanisms for the nation's intelligence agencies have rendered sterling service to Australians. The 2017 review agrees, observing that the current framework constitutes 'a well-structured set of arrangements that provide independent assurance about the legality and propriety of intelligence operations and the management of resources'.

That doesn't mean that the reviewers are content with the status quo. While leaving all of the major building blocks in place, they make two major recommendations for change to the current arrangements. First, recognising the importance of the Inspector-General of Intelligence and Security (IGIS) role—effectively a standing royal commission—they suggest broadening it and increasing the staffing of the office from 17 to 'around 50'. Second, they recommend expanding the remit of the Parliamentary Joint Committee on Intelligence and Security (PJCIS). Both recommendations are predicated on the evolving nature of intelligence work, changes to the composition of the Australian intelligence community and the need for greater public outreach.

The agencies recommended to newly come under the watchful eye of the IGIS and PJCIS are the intelligence elements of the Australian Federal Police, the Department of Immigration and Border Protection, the Australian Transaction Reports and Analysis Centre, and the Australian Criminal Intelligence Commission.

That would certainly make for a bigger workload for the IGIS, especially if it's combined with more public outreach. Whether that all adds up to a need to triple the workforce is impossible to judge on the information provided, though it's also possible that the reviewers thought the IGIS was already understaffed. I won't argue; more oversight resources are a good thing.

The review recommends that the PJCIS's remit be similarly extended to include the agencies listed above. The committee would receive regular briefings from the IGIS, the Independent National Security Legislation Monitor and the director-general of the proposed Office of National Intelligence. However, the operational activities of the intelligence agencies would continue to be outside the purview of the committee—at least as far as formal inquiries go. The review says (paragraphs 7.44 and 7.45) that:

> Rather than giving the PJCIS the power to conduct its own inquiries into agency operations, we favour strengthening the connection between the PJCIS and the IGIS … We recommend that the [Intelligence Services Act] be amended to enable the PJCIS to request the IGIS conduct an inquiry into the legality and propriety of particular operational activities of the [national intelligence] agencies, consistent with the IGIS's remit, and to provide a report to the Committee, the Prime Minister and the responsible Minister.

There's little to argue about in the recommendations made, but there are a few things not mentioned in the review that could usefully be considered in the implementation phase. While not explicitly part of the intelligence oversight framework, other mechanisms play an important role in assuring the public of the propriety of intelligence operations and management. Those include freedom of information processes and recourse to the courts. Neither of those avenues is mentioned in the review. It's hard to believe that everything our intelligence agencies do is sensitive beyond the reach of FOI laws, but there's no discussion of the appropriateness of current blanket exceptions.

Another important—if often imperfect—oversight mechanism not mentioned in the review is the ability of the press to expose questionable behaviour and to ask difficult questions. A related issue is the protection of whistleblowers. There's an undeniable downside to the public release of secret information, but it can also be positive to shed light on improper activities. And it provides a disincentive to cover up misconduct under the cloak of operational security. Edward Snowden's leaks led to press investigations—aided by American FOI laws—that revealed a systematic failure in the oversight of the US National Security Agency. It's true that Snowden leaked far more than that, and I think the net result of his activity was negative. But the case shows that whistleblowing can play an oversight role when all else fails. (And it also shows that constant vigilance is required even when apparently adequate oversight mechanisms are in place.)

I'll finish with one other issue that has been nagging away at me for a while: I can't find a legislative basis for oversight of the activities of the Australian Defence Force's intelligence units. The IGIS oversees the Defence Intelligence Organisation, and the two collection agencies in the defence portfolio are covered by the Intelligence Services Act. But the ADF intelligence elements aren't under the command of DIO and, while carrying our their collection function, they could incidentally gather information relating to Australians. For example, ADF intelligence-collection aircraft might intercept communications from Australians at sea. And there was at least one past instance of a minister instructing the ADF to collect information about Australians—which incidentally provided a good illustration of how the press can help expose infelicities. Perhaps I've missed something (comments welcome), but this looks like a loose end needing tidying—perhaps during the forthcoming legislative review.

For print readers, the original piece with live links is at https://www.aspistrategist.org.au/2017-review-intelligence-keeping-watch/

YouTube series

Justice Robert Hope. Michael L'Estrange: 2017 Independent Intelligence Review https://www.youtube.com/watch?v=G9FFf945F-Y

Intelligence challenges & threats. Michael L'Estrange: 2017 Independent Intelligence Review https://www.youtube.com/watch?v=BuBUwLeie_Q

About the authors

James Clapper was the US Director of National Intelligence, the Cabinet-level official in charge of the US Intelligence community from 2010 to January 2017.

Andrew Davies is senior analyst for defence capability and director of research at ASPI.

Peter Edwards wrote a monograph titled *Robert Marsden Hope and Australian public policy* and is now writing a biography of Hope.

Fergus Hanson is head of the International Cyber Policy Centre at ASPI.

Peter Jennings is executive director of ASPI.

Important disclaimer

About Strategic Insights

Strategic Insights are shorter studies intended to provide expert perspectives on topical policy issues. They reflect the personal views of the author(s), and do not in any way express or reflect the views of the Australian Government or represent the formal position of ASPI on any particular issue.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
Web www.aspi.org.au
Blog www.aspistrategist.org.au

 facebook.com/ASPI.org

 @ASPI_org

ISSN 1449-3993