National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017

I would like to thank the Parliamentary Joint Committee on Intelligence and Security (PJCIS) for the opportunity to comment on this Bill. At the outset I should note that the Australian Strategic Policy Institute does not take corporate positions on any issues. As such the opinions expressed here are my personal views.

The drafters of the Bill should be commended for delivering such a comprehensive modernisation of Australian legislation relating to espionage, foreign interference and secrecy offences. New laws designed to counter sabotage against critical infrastructure and theft of trade secrets are timely and necessary. Indeed, one could argue that the modernisation of our legal framework supporting counter-espionage and subversion was long overdue. So, the legislation is welcome and puts Australia at the forefront of international efforts on the part of the western powers to counter increased activities of a number of states, most particularly China, Russia, Iran and North Korea, to steal intellectual property, threaten the security of critical infrastructure and undermine liberal democracies by subverting their political processes and decision-making sovereignty.

The Bill puts appropriate focus on protecting individual liberties, which ought to address concerns about the legislation's application to the work of journalists and others undertaking legitimate research and open public advocacy. As such, I hope the Joint Committee will provide bipartisan support to the passage of the Bill.

This is complex legislation and the PJCIS can play an important role in supporting the smooth roll-out of these news laws by maintaining a regular focus on their implementation. How the laws are applied will be even more important than how they were drafted. In this context I would like to make five recommendations for the Committee's consideration.

Public awareness and understanding

In a number of media statements over 2017, the Government has stressed that Australia faces an increasing risk of espionage, sabotage and foreign interference. The tone of the public debate would suggest that people are starting to understand that these threats are indeed emerging as a higher risk to Australian security. There is an urgent need for Government, the Parliament and the national security community to find ways to communicate these concerns to the Australian public.[i] It is not easy to bridge the necessary gap between what officials know from classified information and what can be publicly revealed, but Australian officials have for far too long used the veil of national security classifications to avoid making a public case for stronger measures against espionage and subversion.

I recommend that the PJCIS direct the Australian Intelligence Community (AIC) to prepare an annual public report for Parliament on the state of efforts to counter-espionage, sabotage and foreign interference. This could become the basis for an annual Prime Ministerial statement to the Parliament and a debate that might usefully engage the attention of Members and Senators. I acknowledge that the AIC will always be challenged by security classifications in making some information public. However there are good examples from the US, UK and elsewhere where material is put on the public record in the interest of shaping a better-informed public debate. If the threat to Australia's national security is as serious as the Government says, then it's surely reasonable to ask that Parliament makes more information publicly available to strengthen public understanding.

Priorities and resourcing for relevant agencies

The PJCIS should take a close look at the adequacy of AIC resourcing and the priority given to counter-intelligence and counter-subversion work. It is clear that the driving priority for much of the AIC over the last decade and a half has been counter-terrorism internationally and at home. The Agencies will need to address the balance of their efforts between counter-terrorism and the once core business of counter-intelligence. Getting this balance right is critical to successfully implementing the new legislation.

The Committee might note that, on the basis of recent policy statements, such as the United States' 2017 *National Security Strategy* and the unclassified *Summary of the 2018 National Defence Strategy*, key allies and friends are also readjusting the efforts of their intelligence and security agencies to put more weight on countering espionage and foreign interference. The Committee should test whether the AIC has the financial resources and appropriately trained personnel to quickly resume a stronger counter-espionage role.

Links to other Government activities

As the Explanatory Memorandum to the Bill makes exhaustively clear, this new legislation has significant knock-on effects to other parts of government legislation. It is important that the PJCIS examines how well adapted other parts of government are to understand and give effect to the intent of the legislation. For example, the Bill rightly emphasises the need to protect 'privately owned infrastructure' against a range of intelligence gathering and subversion activities. It should be clear to the Committee that this will rapidly involve the work of the Foreign Investment Review Board (FIRB), which in recent years has recommended the government agree the sale of a number of key elements of critical infrastructure – ports, electricity generation and transmission, gas pipelines and large-scale agricultural producers – to foreign entitles. In a number of cases this has included substantial sales of critical infrastructure to Chinese State Owned Enterprises (SOEs) and companies which (whether they like it or not) are closely connected to the Chinese State and Communist Party.

In my view the new legislation makes the current structure of the FIRB untenable. The FIRB operates with an ideological disposition to facilitate foreign investment – as is demonstrated by the tiny (fewer than ten in the last decade) number of foreign investment refusals the entity has recommended compared to tens of thousands of approvals. It seems to regard legitimate concerns about the security of critical infrastructure as confected threat-mongering. FIRB's advice to government is based on analysis and assessment methodologies that are utterly opaque, not least to potential investors.

For the Government's new legislation to work, the time has come to review the governance structures, role and methods of operation of the FIRB. I recommend that the PJCIS should make the FIRB's national security role the subject of a stand-alone review.

Dealing with past decisions on foreign investment in critical infrastructure

The Bill under consideration is closely linked to legislation before the Parliament on the security of critical infrastructure. This is a long overdue but welcome piece of legislation. It points to an emerging understanding of how threats to critical infrastructure are evolving, taking on new dimensions as it relates to cyber enabled industrial control systems and becoming a more prominent focus in the thinking of potential adversaries.

It is encouraging that Australia and a number of key allies and friends are rethinking the security needs of critical infrastructure. Nonetheless, a potentially serious problem emerges as a result of decisions in past years to sell or lease elements of critical infrastructure to foreign entities. We

should be clear here: the problem is not Canadian retirement funds. There is a particular problem around the sale of critical infrastructure assets to Chinese SOEs and so-called private businesses which have to operate within the authoritarian Chinese state-led economy.

I understand that the nature of Australia's economic relationship with China makes this a challenging topic, particularly when so many Australian public and private sector entities have a vested interest in denying there is a problem. It is equally clear though, that Australia and a number of like-minded countries are coming to realise that stronger efforts need to be made to protect critical infrastructure from being used as vectors to engage in espionage, intellectual property theft and sabotage. I suggest that the PJCIS could play an invaluable role by investigating how we manage the consequences of past decisions around the sale of critical infrastructure to foreign entities, particularly from China.

Allied cooperation

Finally, I have mentioned that a number of our key allies and close friends are facing similar challenges relating to espionage and foreign interference. Australia has won some credit for itself in being seen to move decisively to introduce this Bill and other related legislation. I recommend that the PJCIS reach out to counterpart Parliamentary committees – especially among our 'Five Eyes' partners and also Japan, Singapore, France and Germany – to start a wider dialogue on how to counter these evolving threats.

Peter Jennings

Executive Director

Australian Strategic Policy Institute

21 January 2018

[i] The Explanatory Memorandum for the Bill – all 1781 paragraphs of it – sadly fails to clearly explain the broader rationale for the legislation. I appreciate the need to set out a legal interpretation of the Bill, but nowhere does it offer a comprehensible explanation for this substantial piece of policy that would be understandable to a non-specialist audience.