

Submission to the Review of the Defence Trade Controls Act 2012

Thank you for the opportunity to make this submission to the Review of the Defence Trade Controls Act 2012.

ASPI doesn't take a corporate position on any policy matters, so this submission reflects my personal views.

The submission makes 4 major points:

1. Australia's strategic environment has changed markedly since 2012, with direct implications for this legislation and how it operates.
2. Creating Australia's technological edge for our militaries and broader national security communities is a focus for our research community in partnership with government and the defence and tech sectors,
3. Given the strategic change in our environment, it is not in Australia's national interests to enable advancement of the military capabilities of the Chinese state.
4. Research cooperation between Chinese and Australian institutions needs to be regulated to give effect to this policy direction, as this will help protect our nation's future technological edges in areas key to the military and broader national security community.

If this sounds difficult, it is, given that most of the technological areas involved will be dual use, however, focusing regulation on the likely end users (eg. where this is likely to be China's Peoples' Liberation Army or its Ministry of Public Security) will help.

The Defence submission to the Review recommends a new power to regulate, 'where the Australian Government has notified a person that it has reason to believe that the technology is significant to developing or maintaining national defence capability'. This power is being interpreted widely by both universities and defence industry and seen with concern as a result.

Clearer guidance around what is to be regulated and why, as suggested in this submission, may address most concerns within defence industry and so focus effort and debate around the actual national security interests involved.

If closer regulation (and actually saying no to research partnerships and proposals that would advance the Chinese state's PLA or Ministry of Public Security capabilities as a result) sounds politically difficult given the reactions possible from the Chinese government, then it is timely to see that Chinese authorities are proposing to regulate what Chinese researchers can share with foreign partners, including Australian universities. The Chinese state is seeking to protect its future technological edge, with this aligning well with the Chinese authorities' Civil-Military fusion agenda.

Better focused regulation through Australia's Defence Trade Controls Act as proposed in this submission would be a reciprocal regulatory measure to that being undertaken by the Chinese state.

Australia's strategic environment has changed since the Defence Trade Controls Act came into force - the Act needs to change as a result

We now live in a 'post-global world' where the nature of particular states and how they operate matters deeply to how our world works. We have seen the return of states to the heart of international security

and economics. Our governments, officials and business leaders have yet to properly adjust to this post-global world. Some of our political leaders and some in our national security communities see this, however many of our political actors, economic policy makers and business leaders continue to operate as if the inexorable trend towards globalisation is continuing.

This is most evident in policies towards the Chinese state, but also in the actions of the Russian state under Vladimir Putin.

On China, in Australia's case, there is a strong attachment to the policies of the past globalisation era: the approach of focusing our relationship on areas of mutual benefit and not on our differences.

That worked well for both the Chinese state and for Australia when China's focus was on economic growth and its 'peaceful rise'. Now that China has risen, it is beginning to use the power it has built in ways that matter directly to Australia. It is also using state power internally in repressive ways against its own people, enabled by new technologies and mass data collection. Early experience shows that the Chinese state is willing to be a coercive power whose actions are quite different to its public diplomacy language of 'win win' and non-intervention.

China's militarization of the South China Sea in the face of President Xi's commitment to not do this is a stark example. Pressuring international airlines like Qantas to change how they refer to Taiwan to conform with Chinese Communist Party terminology is another example of state coercion, in that case in the realm of commerce. President Xi's reassertion of Chinese Communist Party centrality in decision making economically, strategically and politically is a further indicator.

That coercive use of power will only grow if it is not opposed, called out and frustrated. In the words of the US National Security Strategy, the Chinese state is a revisionist power asserting power through an all of nation long term strategy.

So, while we can still pursue mutual benefit in many areas of economic cooperation with China, we can no longer ignore the differences between the Chinese state and ourselves—because the differences are becoming starker and the differences matter to our security, our stability and our sovereignty. We cannot enable the growth of Chinese military power or enable the Communist Party's internal security agencies to deepen their repressive social control of the Chinese people.

Opposing, calling out and frustrating Beijing's attempts to use power coercively involves risk. However, it is the best path to achieve the future relationship we want: one, if not based on shared strategic interests, at least based on understanding and non-aggression with habits of military engagement and escalation control.

The national debate on China has become unhealthily polarized. It needn't be, because having a strong economic relationship with our major trading partner and protecting our security interests are not mutually exclusive.

Shaping our new policy will be a difficult shift in both the US and Australian governments' relationships with the Chinese Communist Party. In Australia's case, it will involve our political leadership establishing a clear consensus between the major parties on the new principles which will govern our relationship with the Chinese state.

We might have two core principles:

- To engage the Chinese state positively economically and politically, welcoming positive contributions to global prosperity and security, and
- To oppose the Chinese state's development and use of coercive power.

The principles will include careful management of how we communicate about and with the Chinese state—but we need to recognise that the coercive actions we have begun to see and experience are the problem, not the fact that we have noticed them.

So, this is much more than careful public diplomacy, messaging and tone, as that careful public diplomacy has to be based on our clear interests and principles. The principles have direct utility for the Review of the Defence Trade Controls Act.

Creating future strategic and military advantage – critical to protecting Australia and its interests

As it has in the past, future strategic and military advantage is likely to accrue to those who create and apply new technologies. The US and Australia have deep connections in scientific and academic research, and also in defence and intelligence applications of high technology.

Our current military advantage is based on technological and operational dominance, and our military and strategic weight is magnified by working with our international alliance and security partners.

Australian defence and intelligence capabilities contribute to our alliance. At the same time, Australia is critically dependent on the broad access it has to American systems, platforms and technologies to underpin our military and broader Defence organization. The dependence could not be replicated through other relationships. Seeking to be 'sovereign' in creation of indigenous capabilities as an alternative is likely not to be economically or demographically feasible.

However, with the rising economic weight of China and the renewed technical progress of Russia, new sources of technological innovation have arisen which threaten both US and Australian military advantage. This is a new and significant strategic fact which goes to the heart of our alliance and to the heart of how we design and use our militaries. It is a fundamental driver of change in how we approach and regulate research.

Our future alliance's strength will come from the investments our two governments and our corporate sectors make in science and in technological research, along with regulatory and taxation incentives for business and research organisations who engage in relevant research.

It will require us to succeed in translating the relationships between government, our defence industry and our research communities into mastery of emerging technologies—notably technologies of the near and medium term like telecommunications and network technologies, artificial intelligence, quantum computing, autonomy, biotechnology, hypersonics, directed energy, nanotechnology and new materials.

The rise of new centres of technological innovation to which we do not have access means we cannot create this future technological advantage with current practices and relationships.

Many of the required areas of technological advantage involve the tech sectors in our two countries—small start ups and household names like Amazon, Apple, Google and Facebook. The relationship between our governments, our tech sector firms and our 'traditional' defence industries needs to

become a tightly-integrated partnership when it comes to securing future strategic and military advantage.

At present, our tech sectors and our governments have a warily cooperative approach, with the tech sector advocating individual privacy protection and limited cooperation with law enforcement and intelligence agencies based on case by case needs. Similarly, our governments have a regulatory and compliance mindset towards the tech sector when it comes to national security. Our defence sectors are high technology firms, however they are not yet natural partners of our tech sectors or of our militaries.

Competitors—notably the Chinese state and its tech and defence sectors—have a strategic advantage from the close integration that the Chinese Communist Party leads and demands. Whether it is recognised yet or not by our nations’ tech sector leadership and workforce, this creates a strategic business risk to their continued corporate success and technological leadership. Realising this creates the conditions for the tightly-integrated partnerships we require between the US and Australian governments, our research and tech sectors and our defence sectors.

Those close partnerships will depend on trust between all institutions and individuals involved in the others’ active protection of the valuable knowledge and intellectual property that they are creating together. Any constraints to cooperation with the research communities, tech sectors, defence sector and government agencies that the Defence Trade Controls Act might pose should be assessed critically and removed as far as practicable. This will make most sense if US policy makers and regulators make similar decisions on US controls. How the US implements the decision for Australia to be considered part of its National Technical and Industrial base is relevant here.

Our renewed urgency on developing the sources of our future strategic and technological advantage will also require us to adopt much faster cycles of procurement and deployment of military capability. This is not about incremental improvements in capability development lifecycles, or streamlining existing business processes—worthy goals that are valuable when it comes to acquiring traditional large platforms and systems.

Securing the sources of our future strategic and military advantage – what the strategic environment means for Defence Trade Controls and the partnership between the national security and research communities

Australia and the US share the most sensitive and advanced technologies we each have as part of the defence and intelligence relationships we have at the heart of our alliance. We protect such capabilities (like stealth platforms) once they exist with great care and effort so that our military advantages are not undercut.

As an example, the JSF is the product of research and development that took place over the last 30 years. It is essential to protect the results of that research and development now that the JSF exists as a military capability.

To achieve this, Australia and the US between us will spend hundreds of millions of dollars securing the supply chains, maintenance facilities and classified data involved in building and operating the JSF over its life. The workforce to maintain and operate the aircraft will have high level security clearances, the

hangars will be able to hold highly classified material and data and the electronic supply and maintenance systems will be cyber-hardened.

It is time we realized that the sources of our *future* strategic and military advantage —the front end research and scientific advances that generate these future technologies—need equal protective effort.

We must act to prevent research relationships within each of our nation’s academic and research institutions from enabling the militaries of other state actors who do not share our strategic interests.

The means for doing this exist in both our nations’ policies and laws because of our commitment to international arms control and counter proliferation regimes. The US National Security Strategy introduces the idea of a National Security Innovation Base. Australia’s Defence Trade Control Act and the US International Traffic in Arms Regulations and Export Administration Regulations allow our governments to control military and dual use technologies and the research that defines them.

This will be controversial in our research communities and involve regulation of dual use areas of research, some of which are subject to regulation now (quantum computing) and others which currently are not (artificial intelligence and autonomy). The other clear areas for focus are listed earlier in this submission.

Dual use technologies like artificial intelligence are difficult to regulate, as the military uses, while critical, are not the dominant ones (self-driving technology is suited to both cars and tanks, for example), so regulation will likely need to focus on the proposed end user nation and involve risk-based assessments made together with the research community and our tech sectors. Our research sector can help by working to understand both their research partners and the actual likely end users of their work.

It is clear from the submissions from universities and other research organisations that the Review has received that they like the current risk-based approach and do not want further controls. That is absolutely understandable given their focus. The working partnership between the Defence Export Controls Office and the research community sounds very positive – a real strength that came out of the Steering Group led by Australia’s Chief Scientist and the willing cooperation from university staff.

A test, though, of the utility of the current controls is whether there have been many (or any) cases where research or cooperation internationally with clear national security uses that are against Australia’s interest have been identified and either prevented or stopped using the Act. I suspect that this either hasn’t occurred or has done so in less than a handful of cases.

In the new strategic environment sketched out above, combined with the Chinese state’s drive to achieve military advantage by close integration of its research, corporate and military institutions (known as [Civil-Military fusion](#)), it is a growing certainty that Australian research partnerships with Chinese counterparts will be directly advancing Chinese military capability. So, future export control decisions on research are also much more likely to involve refusals if the decisions are made in the interests of Australia’s national security.

[The Chinese state is acting to secure its own technological advantages](#). As the linked report says, ‘the draft regulation, the first time China has released national regulations on scientific data, requires all scientific data generated within China to be submitted “by the lead programme entity” to “state data centres” for review and approval before publication.’

‘Under the proposed new Chinese regulation, scientific data may be shared with foreign collaborators in the case of cross-border cooperation or exchanges, except in the case of “state secrets” where special approval is needed from the ministry of science and technology, according to the draft regulation. But academics note that the definition of ‘state secrets’ in China is notoriously nebulous and ill-defined.’

It would be a strategic error for Australia to enable Australian expertise, intellectual property and research to be used by Chinese institutions and researchers who work with China’s military to advance PLA capabilities, while knowing that there will be no reciprocal provision of Chinese research or intellectual property to grow our own capabilities.

Technology controls can slow particular end users obtaining particular technologies, but will not prevent technological dispersion over time. This means that, along with controls, continual investment in creating new sources of advantage is required.

The regulation will reduce our universities and research institutions’ abilities to obtain funding from other nations, notably China, where it is not in our national interests to advance their military capabilities.

Alternative research funding to our universities and research communities is possible from our defence and tech sectors in Australia and the United States, but are likely to be obtainable only if Australian research institutions are securing the resulting work in the ways proposed here. This could be part of the necessary diversification that our universities and research organisations need to make away from increasing dependence on Chinese funding. This diversification is a matter of good business risk management as much as strategy and national interests.

Conclusion

In summary, the review of the Defence Trade Controls Act 2012 is timely and necessary. A clear-eyed focus on the strategic drivers of the legislation will assist in making proposed changes focused and practicable. Done well, changes to the Act and its operation will result in the working partnership between the Defence organisation and Australia’s research and defence industry sectors operating in a collegiate and effective way to advance Australia’s national interests.

Michael Shoebridge



Director – Defence and Strategy

Australian Strategic Policy Institute

Level 2, 40 Macquarie St, Barton ACT 2600

P: 02 6270 5167 M:0400 963 424 michaelshoebridge@aspi.org.au
| www.aspi.org.au | www.aspistrategist.org.au

25 July 2018