SPECIAL REPORT

Defence and security R&D:
A sovereign strategic advantage

Martin Callinan et al.

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

January 2019

ASPI

About the author

Martin Callinan is a start-up founder (2014–2018), a former Policy Director at the Australian Academy of Science (2009–2014) and a former Defence Science Adviser for the Rudd government (2007–2009). He co-authored ASPI's 2015 Special Report, *Defence science and innovation: an affordable strategic advantage*.

Other contributors from government, academia and industry sectors provided expertise, experience and perspective.

About ASPI

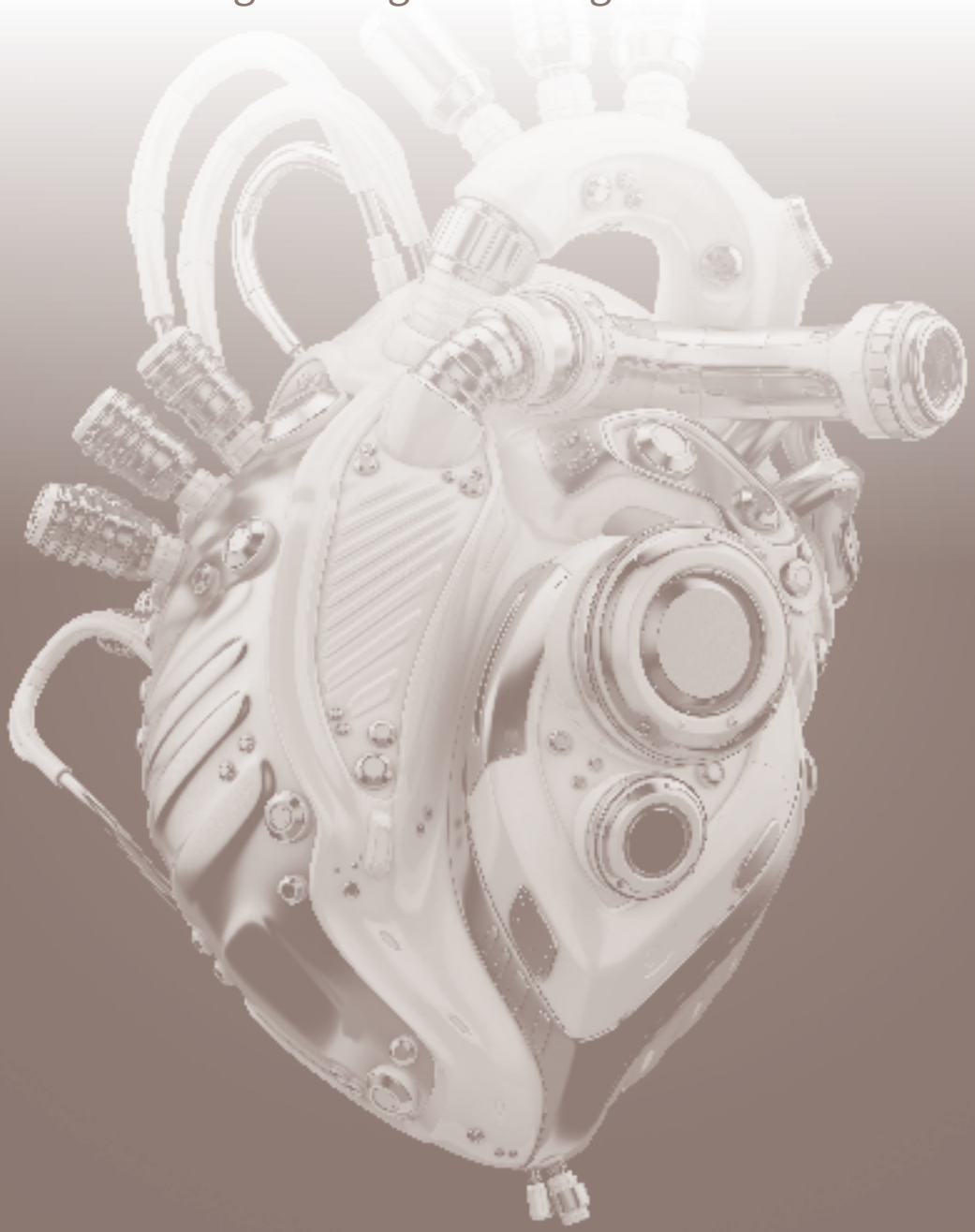
ASPI's aim is to promote Australia's security by contributing fresh ideas to strategic decision-making, and by helping to inform public discussion of strategic and defence issues. ASPI was established, and is partially funded, by the Australian Government as an independent, non-partisan policy institute. It is incorporated as a company, and is governed by a Council with broad membership. ASPI's core values are collegiality, originality & innovation, quality & excellence and independence.

ASPI's publications—including this paper—are not intended in any way to express or reflect the views of the Australian Government. The opinions and recommendations in this paper are published by ASPI to promote public debate and understanding of strategic and defence issues. They reflect the personal views of the author(s) and should not be seen as representing the formal position of ASPI on any particular issue.

Cover image: Sci-fi robotic heart engine, 3d rendering: iStock photo/Vladyslav Otsiatsia.

Defence and security R&D:

A sovereign strategic advantage



Martin Callinan et al.

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

January 2019

First published January 2019

Published in Australia by the Australian Strategic Policy Institute

ASPI
Level 2
40 Macquarie Street
Barton ACT 2600
Australia

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

 Facebook.com/ASPI.org

 @ASPI_org

CONTENTS

EXECUTIVE SUMMARY

Australia's defence, intelligence and domestic security interests are supported by dated and disparate research and development (R&D) policies. This is a problem because global science and technological (S&T) trends are changing in ways that have serious social, security and defence implications. In this emerging contest between our major trading partners, allies and strategic competitors, the high ground to be shared or denied is competitive creation and access to disruptive technological capabilities.

As our strategic outlook deteriorates,[1] there are specific S&T implications that suggest national security R&D policy needs to leverage all of Australia's R&D strengths and evolve into a systematic, collaborative mission involving all national security functions. As global R&D expenditure approaches US$3 trillion, Australia's national security R&D policy settings need to cooperatively engage the whole of government, academia and industry sectors, and those of our allies.

In 2011–12, we allocated 2.4% of our defence budget to R&D. While the defence budget has grown, the R&D proportion is budgeted to fall to 0.98% by 2021.[2] Recent defence innovation policy has significantly improved ambition and engagement, and with it sector culture, but scope and investment remain too modest. The 2017 Independent Intelligence Review identified a critical need for better interaction between the intelligence community and the broader S&T community. Reassuringly, the Australian Government accepted the review's recommendations to realise systematic and coordinated R&D engagement. This recommendation is applicable to the Department of Home Affairs, which was established in part to respond to 'the development of new and emerging technologies'.[3] As the portfolio consolidates, consideration should be given to portfolio R&D and explicit R&D functions within the portfolio. By comparison, the US Department of Homeland Security has a Science and Technology Directorate.

Meanwhile, in their gross national R&D expenditure, authoritarian nations collectively are approaching parity with the sum investment of the Five Eyes nations.[4]

In mid-2018, a joint ASPI – Australian Industry Group (AI Group) survey of firms and higher education and research entities about R&D in support of defence, intelligence and home affairs interests was undertaken. The survey found that, while industry and academia were strong in their praise for the government's 2016 Defence Industry Policy Statement, the budgeted (2018) tightening of the R&D tax incentive raised concerns about government commitment, which hinders R&D planning. Respondents highlighted a lack of significant capability policy and priority development, especially within the intelligence community and the Home Affairs portfolio—and without clear advice it's difficult to engage meaningfully on future requirements. Respondents also expressed concern that departments continue to approach their future technology requirements from an internal demand perspective rather than according to the new R&D engagement policies.

Despite the diminishment of Australia's general S&T advantages by globalisation, current policy is to reduce investment in national R&D, with corollary impacts upon R&D specific to national security. While investment has declined, recent innovation policy (such as the National Science and Innovation Agenda and Defence Industry Policy) are beginning to address longstanding low levels of government–industry–academia collaboration and support for private-sector engagement. In addition to strategically relevant levels of investment, a similar policy refresh is needed for national security R&D.

An efficient whole-of-government response to emerging S&T trends and national security challenges can be developed by systematising government engagement with Australia's broader R&D ecosystem. To help, this Special Report suggests policy options to update, unify and coordinate national security R&D policy:

1. **An Australian Advanced Research Projects Agency**

- Establish a national security Advanced Research Projects Agency similar to US models to fill the R&D gaps in the national security portfolios. With a budget of ~$300 million p.a. (benchmark expenditure proportionate), the agency would provide a critical mass of early-stage, transformative R&D investment.

2. **National security innovation hubs**

- Broaden the scope of the Defence Innovation Hub. With a budget of at least $100 million p.a., it should include functions similar to those of the US Defense Innovation Unit and the US National Security Technology Accelerator (MD5). Those functions speed up innovation processes and build trust between government and non-traditional S&T solution providers.
- Establish an Intelligence Innovation Hub.
- Establish a Home Affairs Innovation Hub. With a budget of at least $50 million p.a., it should be established along the lines of the Defence Innovation Hub recommendation to deal with Home Affairs' broader portfolio responsibilities.

3. **Whole-of-government coordination**

- Combine existing national security departments' and agencies' S&T advisory arrangements, and augment them as necessary, to form a National Security S&T Advisory Committee to jointly service the Defence, Intelligence and Home Affairs portfolios. Following models in the US and the UK, eminent scientists, engineers, technologists and entrepreneurs would provide advice and review services.
- Establish S&T directorates within the Office of National Intelligence and the Department of Home Affairs with a remit to administer S&T policy and activities within their respective portfolios.
- Develop a strategic plan for national security R&D human resources. The plan would be developed collaboratively between government, industry and research entities and cover personnel training pipelines; career paths; security clearances; intrasector mobility; gender and diversity; qualifications; and allied and sectoral exchanges.

4. **Reset national security R&D priorities**

- Review priorities across all government R&D delivery and grant agencies with respect to national security. National security, as appropriate according to whole-of-government objectives, needs to appear at some level in all government research investment priorities. Similarly, special taxation treatment should be afforded, at some level, to industry R&D related to national security.
- Further investment (~$200 million p.a.) in strategically relevant basic fields (including R&D infrastructure) is needed to make a difference significant enough to stop the erosion of Australia's defence and security technological advantages. Consideration is needed to determine what constitutes critical-mass investment to sustain and grow Australia's technological advantage over the long term.
- Develop a national security artificial intelligence strategy, enabled by a critical mass of R&D investment and an implementation program.
- To enable national security R&D sector-wide coordination, consideration should be given to the annual publication of a national security R&D guidance document, including capability forecasts, that industry and academia can use to develop capacities to bring forward new research ideas and solution sets.

INTRODUCTION

This report builds on the 2015 ASPI Special Report, *Defence science and innovation: an affordable strategic advantage* and takes account of domestic and international policy and investment changes since then. The 2015 report argued that global research and development (R&D) trends presented new challenges to Australia's defence. We suggested that our defence science and technology (S&T) arrangements and policy settings needed to be updated. We argued that evolving challenges to our national defence—underfunding and an over-focus in recent years on operational, procurement and sustainment R&D—were diminishing our capacity to undertake, and defend against, transformational and disruptive innovation.

To improve our bang-for-buck, we suggested that defence R&D ought to be managed in a similar way to materiel acquisition: according to clear, strategic, long-term need. We suggested that, in addition to current obligations, the Defence Science and Technology Organisation (DSTO) should return some focus to strategic R&D that is uncontestable from a commercial, secret and academic perspective. Equally, we suggested that significantly increased (funded) collaboration with academia and industry was necessary. We suggested that the US Defense Advanced Research Projects Agency (DARPA) was a suitable model with which to make the most of Australia's considerable innovation capacity.

The government has since released:

- the 2015 National Innovation and Science Agenda
- the *2016 Defence White Paper*
- the 2016 Defence Industry Policy Statement
- the *2017 Foreign Policy White Paper*
- the 2017 *Independent Intelligence Review* report
- the 2018 response to the 2017 *Australia 2030: prosperity through innovation* report
- the 2018 response to the 2016 Review of the R&D Tax Incentive
- the 2018 Defence Export Policy
- the 2018 response to the 2016 National Research Infrastructure Roadmap Research Infrastructure Investment Plan
- the 2018 National Security Science and Technology Policy and Priorities.

It has also handed down three federal budgets (2016, 2017, 2018). Machinery-of-government changes of relevance include the establishment by conglomeration of the Department of Home Affairs (2017) and the establishment of the Office of National Intelligence (2018). Within the Defence portfolio, the DSTO was reordered (2015) as the Defence Science and Technology Group (DSTG), while the status of the Australian Signals Directorate was changed to that of a statutory agency (2018).

This 2019 Special Report's scope is broader, encompassing whole-of-government national security R&D matters. In addition to updating data and policies considered in the 2015 Special Report, security and intelligence R&D matters are also reviewed. To inform consideration about recent progress, particularly on industry and academic collaboration, Australian industry and academia were surveyed in mid-2018 about national security R&D policy and practices.

The following sections provide:

- a description of the global R&D context
- an examination of R&D for national security
- ASPI – Ai Group National Security R&D Survey results
- a description of national security R&D issues
- a discussion
- conclusions.

THE GLOBAL R&D CONTEXT

In our 2015 Special Report, we noted that global R&D expenditure had doubled since 2000. It has now tripled. In a period of low inflation and despite the 2008–09 global financial crisis, global R&D investment since 2000 has grown on average by 6.8% p.a. The significance of global R&D progress isn't intuitively apparent to policymakers and the public at large, and yet it has profound implications for Australia's prosperity and security.

In dollar terms, the change is clearly big. In 2000, global R&D investment was US$720 billion. In 2018, it was more than US$2.2 trillion.[5] This mega-trend, however, hasn't significantly changed the living standards of the vast majority of Australians. All this new work by millions of innovators using modern infrastructure and the latest tools seems abstract, if considered at all.

There are four reasons why Australia's electoral–policy cycle discounts R&D mega-trends, despite their great medium- to long-term strategic importance.

Technology drivers

The first reason is that more lives than ever are being transformed by technology, albeit outside Australia. Since 2000, the deployment of new technology has underpinned a halving of global child mortality (from 10 million to 5 million p.a.[6]) and a doubling of the global middle class (from ~1.5 billion people in 2000 to ~3.4 billion people[7]). This profound change isn't a current, first-hand experience in a country that surpassed such measures 60 years ago.

The 30 years between 1915 and 1945 saw broad deployment in Western countries of electrification, refrigeration, motorisation, telephony, radio, cinema, cars, trucks, aeroplanes, mass transport, fertilisers, antibiotics, vaccines and high explosives (atomic weapons were used twice). The compounding and improving use of these technologies after World War II underpinned unheralded prosperity, led by countries such as Australia.

This is a proven method; every single country today has policies and programs to innovate. Then, as now, the latest available technology was used where possible to meet national demands. As globalisation has demonstrated, this isn't an evolutionary process or a process necessarily bound by domestic history. Copper-wire telephone infrastructure isn't needed to deploy mobile phone technology. This characteristic of technology dispersal is of strategic relevance as it shows that global R&D outcomes affect all countries' prospects, irrespective of their technological past or the apparent relevance of technological impacts elsewhere.

Social change

The second reason is that, while recent global R&D hasn't greatly altered Australia's physical living standards, the engagement and functions of our society are undergoing extensive and pervasive change. The major innovation over the past 30 years has been the development and deployment of information communication technologies (ICT: computers, the internet, mobile phones, smartphones, tablets, sensors and software, such as automated and autonomous systems). The global economy depends on ICT services and the communication efficiencies they provide, but the most notable change in developed countries hasn't been physical (such as adequate nutrition) but how we connect with information, ideas, family, friends, our broader society and, indeed, the world.

Since the introduction of smartphones a little more than a decade ago, 80% of Australians have bought them. On average, we use social media at least five times a day,[8] adding up to at least 10 hours of access each week. Australia has 17 million active Facebook users, about half of whom log in daily.[9] Broadcast television viewing has dropped in recent years, and 18–24-year-olds now watch more video content on handheld devices than on television.[10]

Enabling this social change have been the fruits of changing global R&D investment patterns. Leading global R&D spending in 2017, by industry sector, was computing and electronics at 23.1%. The software and internet sector accounted for 14.5%. Both these ICT fields eclipse, by an order of magnitude, the 3.2% spent on global aerospace and defence R&D.[11] In 2017, Alphabet/Google, Microsoft, Intel, Apple and Cisco together spent over US$60 billion on R&D.[12] Most of us carry more computational and connectivity capability in our pockets than NASA used to visit the moon 50 years ago.[13] The result of this recent R&D investment facilitates, circumscribes and informs all Australians and our institutions.

Online tasking services (the gig economy, such as Uber and Airtasker) are driving changes to work and living practices historically regulated, arbitrated and integrated into Australia's social contract (for example, the minimum wage and superannuation). Community volunteer hours are in decline,[14] and loneliness is becoming more prevalent.[15] Traditional social structures based on family, employment, schools, sport and geography are changing. New associations are forming according to individual discovery, interest, support, affirmation, short-term employment and opportunities found and sustained online. In turn, national identity and interests are being reshaped by electronic engagement, increasingly focused or arranged by algorithm-directed influences, including the marketing strategies of global advertisers, special interests advocacy and interactive commercial entertainment.

The corporations that facilitate this information control are developing sovereign-like authority and are able to exercise power (public opinion) disruptively or disingenuously by way of disinformation (bias) and misinformation (fake news). Typically, this takes the form of cognitively informed, big-data-focused, strategically targeted advertising. Recent developments in artificial audio and video production technology, whereby hours of (real) source data is used to inform a dynamic, programmable model, can produce (fake) audio and video of sufficient quality to convince informed audiences.

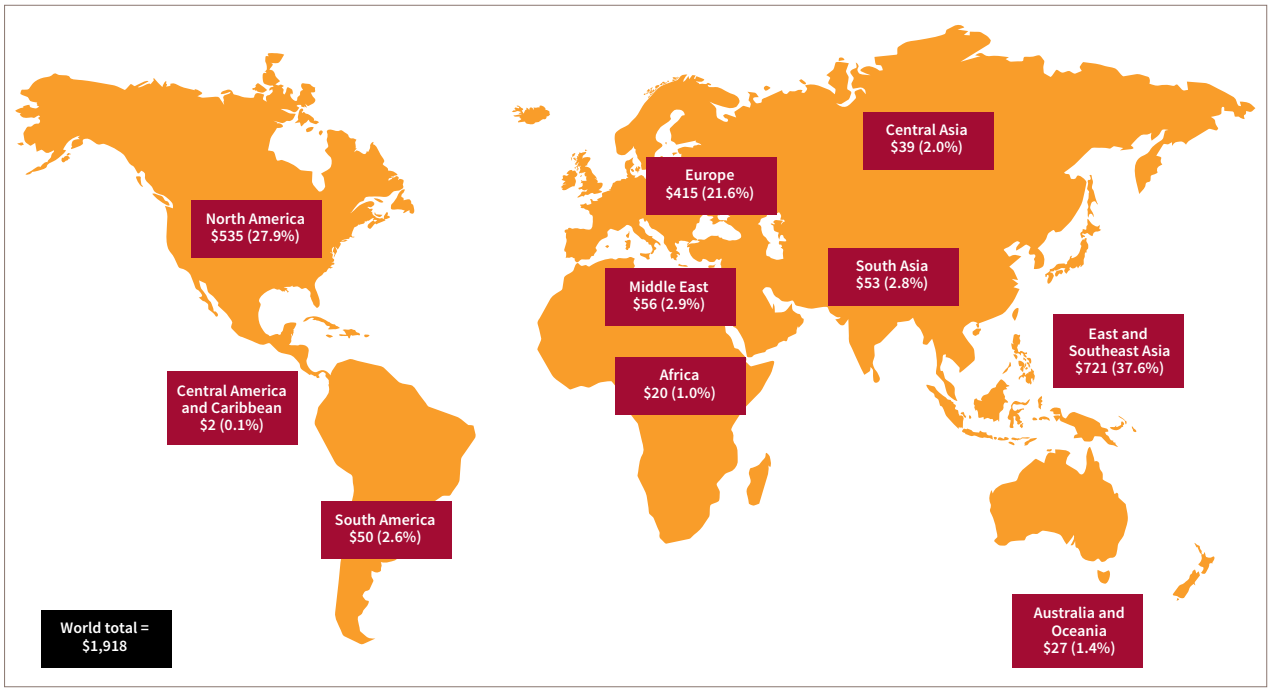
Global R&D investment growth in ICT suggests that these capabilities, and thereby the capacity to transform society, will continue to grow. One consequence will be a growing capacity of non-Australian actors to influence our national awareness, seeking to intervene in, or at least influence, democratic processes, such as public debate, elections and representation. This presents a novel challenge to our national security. As an emerging threat vector, it sits outside the traditional scope of government control.[16] The recent foreign interference within Australian universities is a symptom of his trend.

Changes in the dynamics and mechanisms of Australia's social interaction are strategically relevant because of the sensitive relationship between public opinion and institutional control in a functional democracy. There's already evidence of Australian institutions (such as governments and media) losing social traction,[17] and of growing ambivalence, particularly among younger Australians, about democracy and democratic ideals.[18]

Non-allied investment

The third reason is that most of the recent global R&D growth has come from non-allied countries. While this investment has a focus on economic development, as their economies and innovation ecosystems mature, so too does their capacity for basic research.[19] As shown in Figure 5, global 2015 R&D expenditure in East and Southeast Asia accounted for 37.6% of the global total. North America accounted for 27.9%, Europe for 21.6% and Oceania for 1.4%.

Figure 1: Global R&D expenditures, by region, 2015 (US$ billions, PPP)



Twenty years ago (in 1996–97), China's gross expenditure on R&D (GERD) was US$21.1 billion at purchasing power parity (PPP),[20] while Australia's was A$8.8 billion.[21] By 2017, China's expenditure had grown to US$429.5 billion,[22] while Australia's had grown to A$31.2 billion (2016).[23] In 1997, Australia had a clear comparative advantage based on decades of high-quality research investment. China's GERD at the time was focused on heavy industrial development. In 2005, China had one university ranked in the world's top 200, compared to Australia's six.[24] By 2017, Australia had 10, while there were nine in China.[25]

Between 2007 and 2017, the US increased R&D expenditure by 43%, to more than US$525 billion (PPP), but over the same period its share of global R&D fell from 32% to 25%.[26] Australia's GERD decreased by 7% between 2013–14 and 2015–16. As a proportion of GDP, our GERD peaked in 2008–09 at 2.25%. By 2015–16, it had fallen to 1.88%.[27]

Compared to the innovation systems of other countries, Australia's R&D sector has particular strengths and weaknesses. Mirroring AT Kearney's 2018 Global Innovation Index, the Bloomberg 2018 Innovation Index ranked Australia 20th (Table 1).[28] The breakdown of that ranking reveals that a comparative strength is 'researcher concentration' (we were 3rd). This indicates that we're world leading in terms of researchers per population. International ranking of 'research' output confirms our research performance as being among the world's best. However, we ranked near last for 'development' outputs, and our academic–industry collaboration rates ranked near last in the OECD.[29]

Table 1: Bloomberg 2018 Innovation Index

2018 rank	2017 rank	YoY change	Economy	Total score	R&D intensity	Manufacturing value added	Productivity	High-tech density	Tertiary efficiency	Researcher concentration	Patent activity
1	1	0	S Korea	**89.28**	2	2	21	4	3	4	1
2	2	0	Sweden	**84.70**	4	11	5	7	18	5	8
3	6	+3	Singapore	**83.05**	15	5	12	21	1	7	12
4	3	–1	Germany	**82.53**	9	4	17	3	28	19	7
5	4	–1	Switzerland	**82.34**	7	7	8	9	11	17	17
6	7	+1	Japan	**81.91**	3	6	24	8	34	10	3
7	5	–2	Finland	**81.46**	8	16	10	13	19	6	4
8	8	0	Denmark	**81.28**	6	15	11	15	26	2	10
9	11	+2	France	**80.75**	12	35	14	2	10	21	9
10	10	0	Israel	**80.64**	1	27	9	5	41	1	19
11	9	–2	US	**80.42**	10	23	6	1	42	20	2
12	12	0	Austria	**79.12**	5	8	15	26	12	12	5
13	16	+3	Ireland	**77.87**	22	1	1	18	20	14	33
14	13	–1	Belgium	**77.12**	11	22	13	10	37	13	21
15	14	–1	Norway	**76.76**	19	37	19	11	23	8	14
16	15	–1	Netherlands	**75.09**	17	26	20	6	47	15	18
17	17	0	UK	**75.54**	20	40	23	14	8	18	15
18	18	0	Australia	**74.35**	14	46	16	17	17	3	20

The primary product of the past 30 years of global R&D has come predominantly from allied nations. While Australia's utilisation of and contribution to this aspect of globalisation has not been insignificant (CSIRO developed Wi-Fi, and our public education standards allow the ready adoption of new technologies), we've been close-following beneficiaries of US-led innovation.[30]

Apart from New Zealand, these are not the circumstances of our regional neighbours, or most of the world. Poverty alleviation, scarce natural resources, population pressures and strategic interests have informed policy settings to maximise national technological advantage. China's R&D expenditure has increased on average by 18% p.a. since 2000. Its innovation ecosystem is starting to produce novel, scalable enterprises. In 2017, Chinese start-ups and new tech firms attracted a record US$58.8 billion in finance rounds, including heavy investment in series D (advanced) start-ups.[31] As of mid-2018, China had more than 160 'unicorn' companies.[32]

Non-allied governments and their private sectors, led by national policy, are leading this growth in investment scale and strategic purpose. The proportion of global R&D by OECD nations dropped from 80% in 2000 to 61% in 2016.[33] In 2017, the Five Eyes nations constituted 31.2% of global R&D, whereas the US alone contributed 33.2% in 2000.[34]

Unlike the innovation profiles of our larger allies, Australia's profile (leading research capability with a lagging development capability) is the opposite of the innovation profile of authoritarian nations. Australia has a comparative advantage in the creation part of the technological development path (research[35]) but, ultimately, it's the use and control of new applications (development) that delivers strategic value.

Sustained non-allied R&D investment is strategically relevant because the sheer volume (about 20 times Australia's total investment) of new R&D activity to solve topical problems will inevitably produce new knowledge.[36] Given their development and application focus and experience, novel capabilities and businesses should be expected. Even though the US continues to lead R&D in every major industry (except the automotive industry, where Japan now leads), the weight of strategic investment elsewhere means that the clear technological supremacy that Australia and our allies enjoyed all last century is not set to continue through much more of this century. As James Clapper, a former US Director of National Intelligence has noted:

> The consequences of innovation and increased reliance on information technology over the next few years on both our society's way of life in general and how we in the intelligence community specifically perform our mission will probably be far greater in scope and impact than ever … These developments will pose challenges to our cyber defenses and operational tradecraft but also create new opportunities for our own intelligence collectors.[37]

Time matters

The fourth reason is that the time available to detect and react to technological developments is decreasing, and in doing so diminishes our institutional responsiveness. This phenomenon is difficult to measure, and our electoral–policy processes struggle to accommodate its consequences. Hastened particularly by improving ICT services and, increasingly, by autonomous systems, the real-time provision of massive amounts of information is compressing decision-making cycles. Whether the issue is IT system disruption, Mach 5 travel (Melbourne to Perth in 26 minutes), electoral distortion, infection rates or disruptive enterprise, the temporal consequences of recent R&D investment challenge the ability of policy setters and decision-makers to control or direct effective responses.

As tech adoption, integration and recombination (such as the internet of things) continue, deliberative decision-making will increasingly depend upon preparedness. Reduced decision-making time is strategically relevant because competitive advantage depends upon the amount of time available to both make and carry out feasible decisions. This emerging technological dynamic contributes to Paul Dibb and Richard Brabin-Smith's argument that the prospect of shortened warning times now needs to be a major factor in today's defence planning.[38]

Consequences for Australia

On scale alone, these four trends will have a material impact in the medium term. If the international R&D trends of the past 18 years continue for the next seven years, global R&D expenditure will top US$3.4 trillion p.a. around 2025. Assuming Australia maintains sub-inflation R&D investment to 2030, our proportion of global R&D investment will drop to less than 1%.[39] We noted in our 2015 Special Report that Australia produced 3% of the world's research, which receives 4% of world citations, thanks to historical investment and research excellence. By 2030, both those productivity indicators may approach 1%.

As developing and transitioning nations continue to build upon their success, our proportional R&D output will decline, along with our comparative capacity to manage the impacts of technological innovation produced by the rest of the world. The challenge for Australian policymakers is how to maintain competitiveness in the light of booming technological speciation, as an ever-greater number of ever more various ideas are realised and compete for survival.

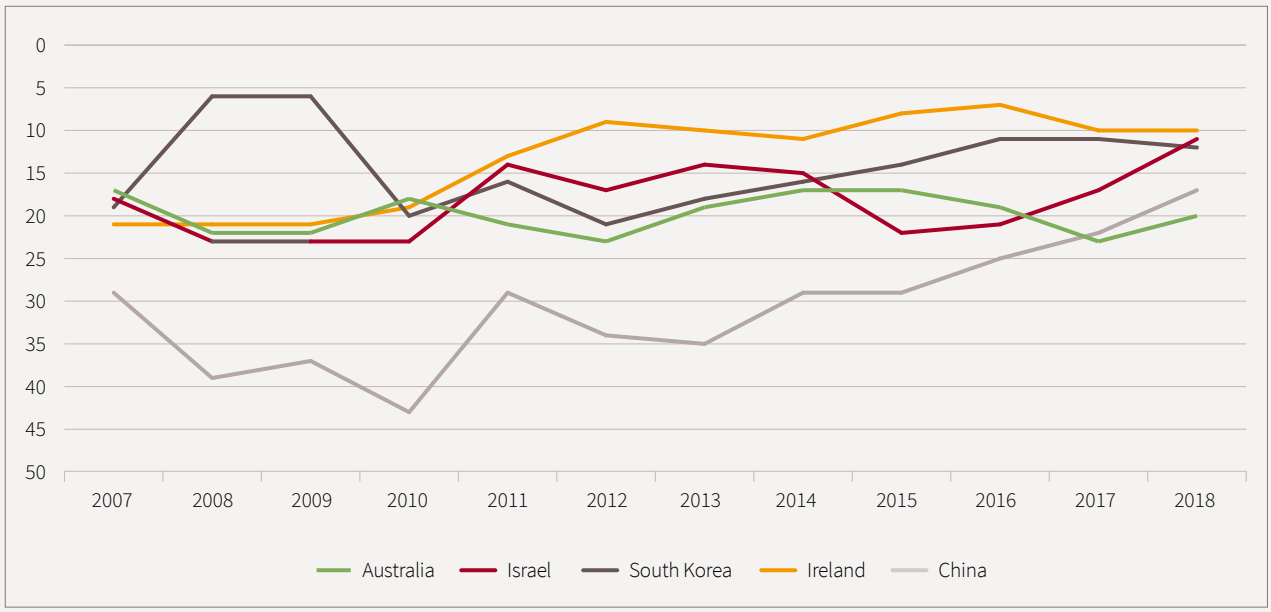
As the implications of these global trends are difficult to predict, it's prudent to prepare means by which to manage the scale of tech-driven change that's certain to come. Fortunately, and rare among the world's nations, we've several decades of quality investment in intellectual capability to do so.

R&D FOR NATIONAL SECURITY

Gross Australian expenditure on R&D as a proportion of GDP declined from 2.25% in 2008–09 to 1.88% in 2015–16,[40] and expenditure on R&D performed by state and federal government agencies fell to $3.279 billion in 2016–17 from a high of $3.42 billion in 2008–09 in current price terms.[41]

Our international innovation standing reflects this trend. AT Kearney's 2018 Global Innovation Index (GII) uses 82 indicators (58 hard data, 19 composite indicators from international agencies and 5 responses to World Economic Forum surveys). Co-authored by Cornell University, INSEAD and the World Intellectual Property Organization, the GII provides an annual high-level view of innovation performance across some 130 economies. For the seventh consecutive year, Switzerland led the rankings, followed by other advanced European nations, the US and Singapore (Figure 2). Australia can and should be in this grouping.

Figure 2: AT Kearney Global Innovation Index rankings, selected countries, 2007 to 2018



Source: AT Kearney, Global Innovation Index, 2018, online.

For political, business, scientific and academic decision-makers in Australia, the GII reports give pause for thought. Over the past decade, Australia's ranking has hovered between 17 (2017) and 23 (2017), and is currently 20. However, peers who were trailing us in 2007—Israel (18), South Korea (19) and Ireland (21)—dramatically improved their rankings by 2018 (to 11, 12 and 10, respectively). In fact, the OECD average R&D investment per GDP has increased over the past decade. Over the same period China, has improved from 29 to 17.

R&D in Australia's defence community

This pattern of real and relative decline is mirrored in the performance of Australia's defence R&D. In the 2015 Special Report, we noted that total expenditure on defence R&D had fallen steadily since 2011 and that the government R&D share of the overall defence budget had dropped from 2% in 2008–09 to a forecast (2015 budget) 1.1% in 2017–18.

Updated statistics from the Australian Bureau of Statistics (ABS) and Defence Portfolio Budget Statements indicate that government defence R&D as a percentage of the defence budget continues to decline, and is now budgeted to be less than 1% (0.98%) by 2020–21 (Table 2).

Table 2: Defence and Defence R&D (DSTO/DSTG) expenditure, selected years, 2000–01 to 2020–21

Year	Defence budget ($m)	Total defence R&D ($m)	Govt defence R&D ($m)	Govt defence R&D (% defence budget)	Business defence R&D ($m)	Business share of defence R&D (%)
2000–01	14,453	401.1	238.6	1.6	158.1	39.4
2004–05	20,569	616.6	309.3	1.5	278	45.1
2008–09	24,081	800.9	486	2	259.4	32.4
2011–12	26,320	795.9	598.8	2.3	197.1	24.8
2012–13[a]	26,940	n.a.	553.8	2.1	n.a.	n.a.
2013–14	27,110	663.9	421.2	1.5	242.7	27.35
2014–15	29,302	n.a.	416.5	1.4	n.a.	n.a.
2015–16	31,863	651.4	463.9	1.4	187.5	28.8
2016–17	32,382	n.a.	447.5	1.3	n.a.	n.a.
2017–18	35,191	n.a.	473	1.3	n.a.	n.a.
2018–19	36,452	n.a.	475	1.3	n.a.	n.a.
2019–20	39,245	n.a.	405.8	1.1	n.a.	n.a.
2020–21	42,565	n.a.	420.2	0.98	n.a.	n.a.

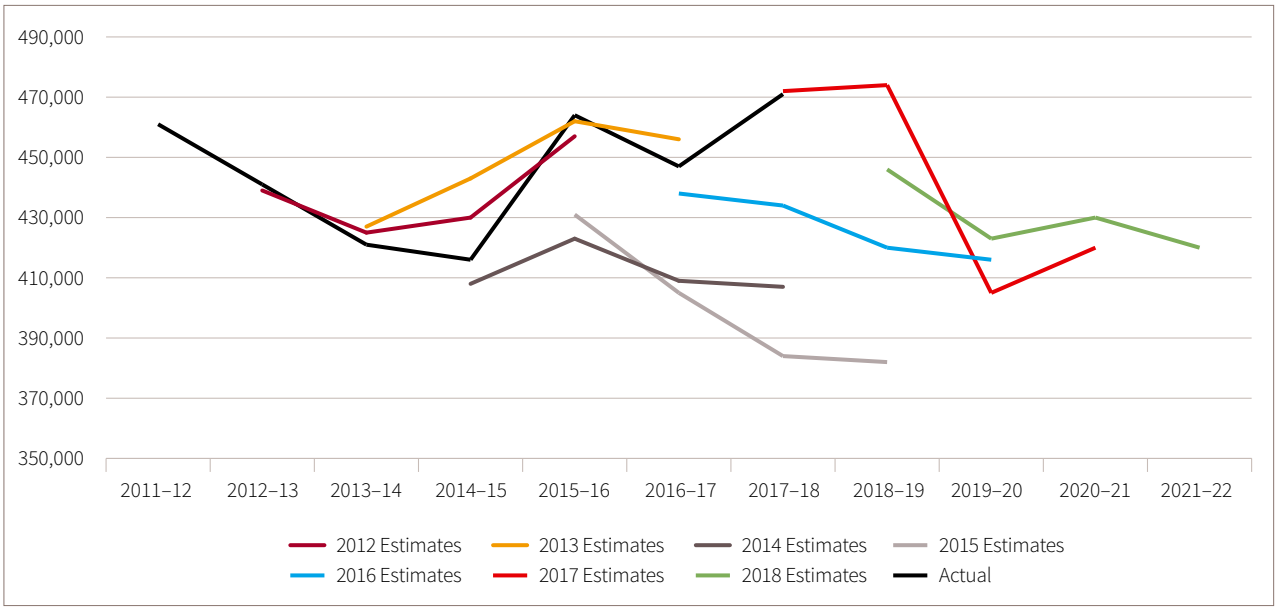
DSTO/DSTG = Defence Science and Technology Organisation / Defence Science and Technology Group.

[a]The ABS cut collection and publication from annual to biannual.

Sources: ABS, cat. nos. 8109.0, 8104, various; Defence Portfolio Budget Statements.

Projections at the national security R&D agency level (DSTO/DSTG) follow a similar pattern. Estimates in 2014, 2015 and 2016 planned for significantly reduced expenditure, although actual spending to 2016 followed 2012 and 2013 estimates. This disconnect suggests strategic planning conflicts that, despite a (non-forecast) ~$20 million increase in 2016, may have been resolved. This is because since 2014 all Budget estimates have depicted cuts; for example, the current Budget forecasts a ~$50 million reduction over the forward estimates (Figure 3). Budget reductions have been realised in large part through a 20% staff reduction during the past several years. In 2011, DSTO had approximately 2,500 staff, which dropped to 2,300 by 2013–14[42] and to 2,055 in 2018.[43]

Figure 3: Budget estimates for DSTO/DSTG, 2011–12 to 2021–22



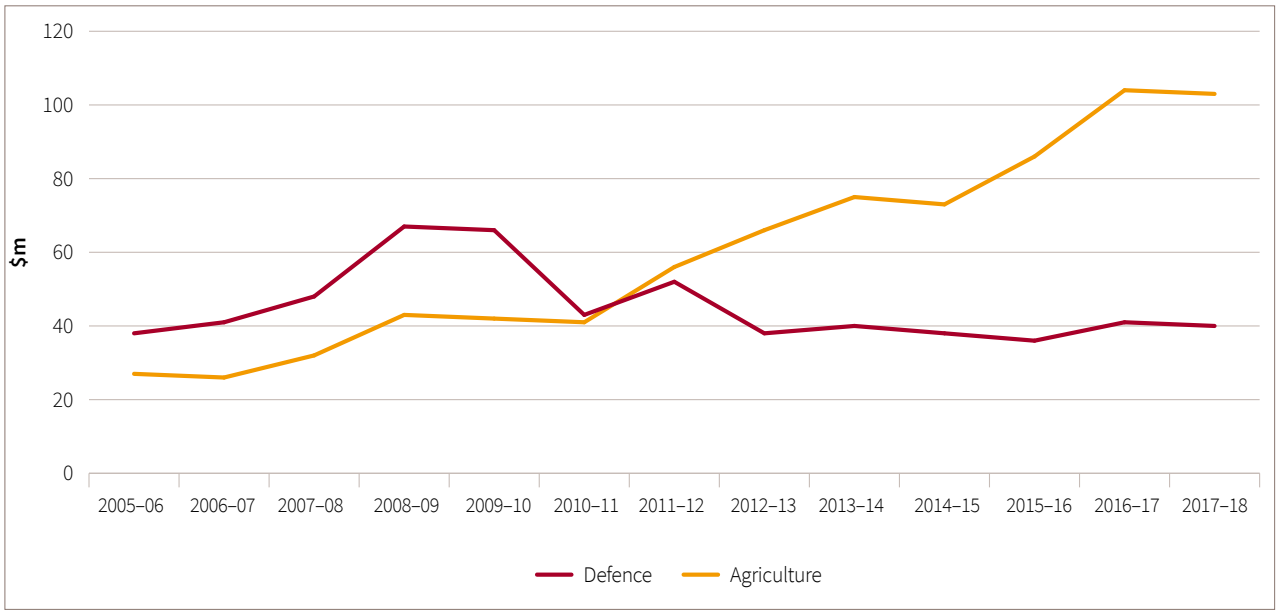
The 2016 Defence Industry Policy Statement reformulated existing innovation support efforts under two 10-year programs:

- The Defence Innovation Hub ($64 million p.a.) incorporated the Capability Technology Demonstrator program ($15 million p.a.), Rapid Prototyping Development and Evaluation, and the Defence Innovation Realisation Fund managed by Defence's Capability Acquisition and Sustainment Group.
- The Next Generation Technology Fund ($73 million p.a.), incorporating funding for the Trusted Autonomous Systems Cooperative Research Centre ($50 million invested over seven years), is managed by DSTG.

Declines in government defence R&D haven't been matched by commensurate increases in business defence R&D. The ABS reports that in 2015–16 the business share of defence R&D had fallen to 28.8%. This was down from a high of 45.1% in 2004–05.

This pattern of decline or, at best, this stagnant level of business investment in defence R&D is also evident in the 2017–18 statistics released by the Department of Industry, Innovation and Science detailing defence firms' use of the R&D tax concession. The performance of the defence business sector on a 2017 constant dollar basis stands in stark relief when compared, for example, with the use of the R&D tax concession by firms in Australia's agriculture sector (Figure 4). Australian business expenditure on engineering R&D fell from $9.2 million to $5.5 million between 2010–11 and 2015–16.[44]

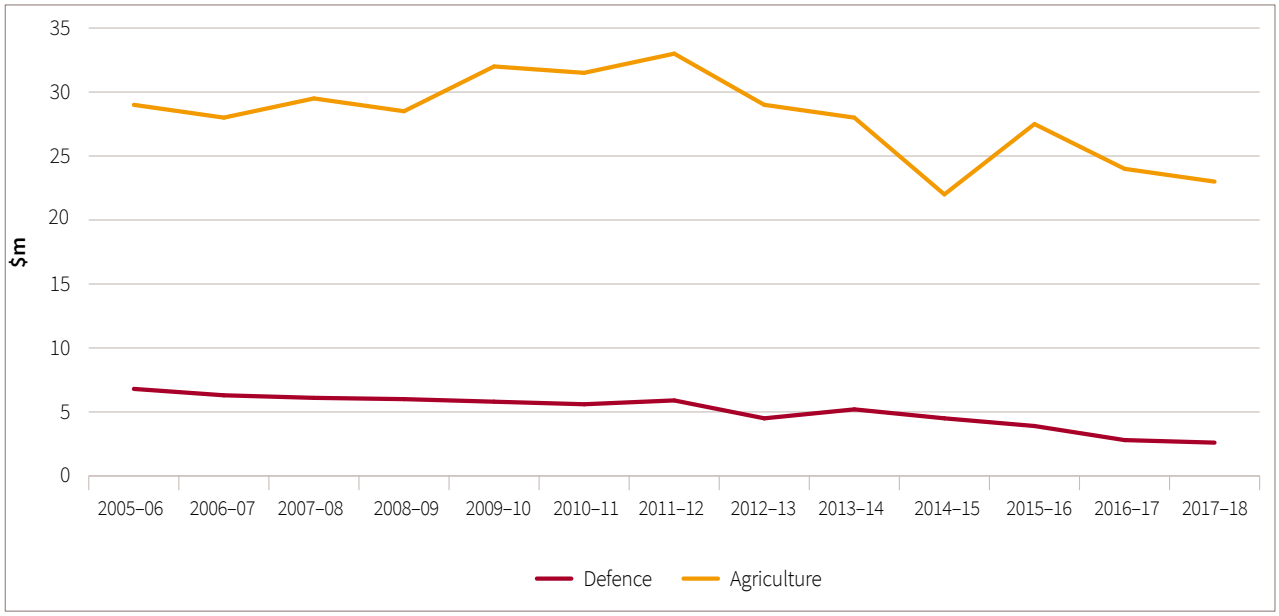
Figure 4: Comparison of use of R&D tax concession by firms in the defence and agriculture sectors, 2005–06 to 2017–18 (constant 2017 $ millions)



Source: Department of Industry, Innovation and Science (DIIS), 2017–18 SRI Budget Tables and Reserve Bank Inflator calculator.

University defence research funding is also lagging. In our 2015 Special Report, we noted falling levels of investment by the Australian Research Council (ARC) at the time of the discontinuation of the 'Safeguarding Australia' research priority. The latest data from the Department of Industry, Innovation and Science shows a steady decline in ARC investment in defence-related activity (Figure 5). In 2017–18, the amount allocated by the ARC to defence-related activity represented 0.4% of the ARC's total budget.

Figure 5: Comparison of Australian Research Council allocations to defence and agriculture sectors, 2005–06 to 2017–18 (constant 2017 $ millions)



Source: DIIS, 2017–18 SRI Budget Tables and Reserve Bank Inflator calculator.

The ABS reported in May 2018 that the overall level of R&D performed by the higher education sector as a proportion of GDP was steady: 0.63% in 2014 to 0.62% in 2016.[45]

Almost a third of higher education R&D investment was devoted to fields of research in the medical and health sciences domain ($3,087 million or 28%) in 2016. In total, the fields of medical and health sciences, engineering, biological sciences and studies in human society made up just over half (53%) of total higher education R&D investment ($3,087 million, $1,115 million, $1,021 million and $497 million, respectively). These top four fields of research, in terms of expenditure, remained consistent between 2014 and 2016.

R&D in Australia's intelligence community

The level of R&D undertaken by Australia's intelligence community is difficult to quantify. There are national security considerations behind that reality. The best recent insight can be gleaned from the 2017 Independent Intelligence Review (IIR).[46] The review noted that the budget for the agencies that constitute the Australian intelligence community approached some $2 billion in 2017. The review didn't elaborate on what percentage of that budget was spent on R&D but did make several recommendations to adopt a more structured approach across the agencies to more effectively respond to the challenges and threats posed by 'accelerating technological change'.

The recommendations included:

- establishing a National Intelligence Community Science and Technology Advisory Board
- creating a National Intelligence Community Innovation Fund
- supporting a National Intelligence Community Innovation Hub to facilitate ways in which government, industry and academia could come together to address capability needs and solutions.

The comments and recommendations made by the IIR suggest that, in R&D by the Australian intelligence community, much more could be done beyond the community's own internal technical capacities and what's available through piggybacking on the efforts of the other Five Eyes countries.

There's a fine balance to be struck between revealing too much about different agency budget allocations, which may give an advantage to those seeking to cause harm to Australia or Australian interests, and providing transparency and critical linkages to Australian industry and academia to assist the Australian intelligence community in executing its various tasks.

This perennial tension is shared by the other countries that make up the Five Eyes community, but in several cases, notably the UK and the US, innovative overarching strategies have been put in place that enable their intelligence agencies to engage with industry and academia in a safe, systematic and controlled way. Those approaches merit closer scrutiny by the new Office of National Intelligence.

Reports and public evidence provided by various Five Eyes intelligence leaders to their respective parliamentary institutions suggest that there's a recognition, and a serious concern, that the level and diversity of technological disruption underway around the world has accelerated so much that a less stovepiped and much more joined-up approach is required.

Increasing engagement with industry and academia is seen as essential. In the past few years, various industry and academic engagement initiatives, which don't compromise strict security considerations, have been rolled out by some Five Eyes countries. For example, the UK intelligence community publicly reports via the 'Single Intelligence Account'. With the establishment of the Office of National Intelligence in Australia, there should, *prima facie*, be scope to emulate the UK approach, and perhaps to consider extending the concept to include a disclosed S&T component.

The Department of Home Affairs

In parallel with the release of the IIR, then Prime Minister Turnbull announced the creation of the Department of Home Affairs. Following the passage of enabling legislation in June 2018, the portfolio drew together the former Department of Immigration and Border Protection and the Australian Federal Police, the Australian Border Force, the Australian Security Intelligence Organisation, Emergency Management Australia, the Australian Criminal Intelligence Commission, the Australian Transaction Reports and Analysis Centre, the Office of Transport Security and the Australian Institute of Criminology. In 2018–19, Home Affairs had a budget of some $3.2 billion and some 23,000 employees. However, the Budget was silent on how much the portfolio has spent on R&D or intends to spend over the forward estimates.

Home Affairs acknowledges the 'confluence of technological developments and the threats' Australia faces,[47] yet the Department of Immigration and Border Protection's Research and Innovation Division (established in 2014 to deliver value-added research advice and innovative technology solutions[48]) didn't carry over as a distinct element of Home Affairs' mid-2018 organisational structure. Current resource allocation to R&D appears unchanged from the sum of those of the constituent entities that now comprise Home Affairs. The sum is understood to be significant and servicing a wide range of S&T needs.

The Australian Institute of Criminology researches, funds and collaborates to produce quality, targeted criminology-oriented research. With an annual budget of approximately $7 million, investment in this field would appear to represent more than half of the Home Affairs' total R&D expenditure.[49]

A notable successful collaborative investment is the Data to Decision Cooperative Research Centre, which is supported by several government agencies, including the Australian Federal Police and Home Affairs (through an investment at its establishment by the Department of Immigration and Border Protection). Arguably, the centre's success is moderated by the size of investment (that is, demand for its work appears to be greater than investments to date).

In contrast, the US Department of Homeland Security (with US$40 billion p.a. budget and more than 240,000 staff) has a Science and Technology Directorate with 450 staff and a budget of US$1.1 billion, which includes the Homeland Security Advanced Research Projects Agency (HSARPA).[50] Proportionally, in terms of staff allocation, R&D function and R&D investment, an equivalent Australian department would have 50 staff and an advanced research project capacity and would invest ~$80 million p.a. in R&D.

It's reasonable to expect that Home Affairs' constituent departments and agencies will require concerted R&D support into the future. The level of R&D engagement with industry and academia by the Home Affairs portfolio will need a coordinated methodology or an overarching framework to join national R&D capability with medium- to long-term Home Affairs needs. As Home Affairs' establishment is still a work in progress, there's an excellent opportunity to clarify R&D functions to meet whole-of-department and whole-of-government strategic needs and to provide an internal budget for that R&D.

National security R&D

Existing national security R&D programs and policies reflect existing departmental structures and objectives rather than being an ongoing response to global S&T megatrends. As those trends advance, department-oriented structures begin to date. In recognition of the acute challenges presented by global trends, initial whole-of-government responses have emerged.

The role of the National Security Science and Technology Centre is to coordinate whole-of-government national security S&T; foster academic and industry S&T partnerships; foster international research collaboration; and manage DSTG's national security S&T program.[51] The objectives are reasonable, but the centre's capacity to administer a major whole-of-government policy objective from within the Department of Defence, without line authority and with a budget sufficient to support only a dozen staff, is severely limited.

The National Security Science and Technology Interdepartmental Committee was established in March 2017. It endorsed six national security S&T priorities:

- cybersecurity
- intelligence
- border security and ID management
- investigative support and forensic science
- preparedness, protection, prevention and incident response
- technology foresighting.

Apart from foresighting, the priorities reflect existing departmental challenges, which is reasonable, but they exclude broader and future S&T challenges, such as artificial intelligence and biomedical technologies, which seem likely to be critical to Australia's future security.

In 2018, DSTG published *National security science and technology: policy and priorities* to 'outline Australia's current national security S&T priorities and coordination of efforts, to best take advantage of investment in S&T and address gaps in immediate and future national security capability'.[52] Outlining whole-of-government policy and priorities, the report addresses more of the challenges, although without identifying the ways or means to respond effectively to them.

THE ASPI – AI GROUP NATIONAL SECURITY R&D SURVEY

The ASPI – Ai Group National Security R&D Survey of firms and higher education and research entities (universities, research institutes and cooperative research centres) provided insight into Australian R&D activities and government policy settings in the defence, intelligence and security R&D domains. The mid-2018 email-based survey also sought policy opinions to explore options to improve engagement and productivity.

The confidential nature of the survey required that only generic responses and trends be published; some written responses were further explored in follow-up discussions. The response rates—start-ups (~16%), small and medium-sized enterprises (~30%), multinationals (~16%) and research entities (~33%)—suggest that the survey results may be taken as indicative rather than representative.[53]

This section comments on the survey results.

The 2016 Defence Industry Policy Statement

Firms, universities and other research entities are in no doubt that the 2016 Defence Industry Policy Statement is having a positive impact. A large majority reported that R&D initiatives contained in the statement are having a medium to high level of impact. The government's 'clear articulation of their vision' was widely noted, and the experience has been positive so far.

While firms and universities felt that the ideas and philosophies contained in the statement were correct, a degree of scepticism about the translation of visions to action and follow-through was evident. Firms provided examples of the slowness involved in processing applications. In one example, it took more than nine months to reach a go / no-go decision. A degree of frustration was evident about the lack of substantive feedback, which might assist learning, address weaknesses and improve the chances and value of future collaborative efforts.

Firms were cognisant of the costs involved in preparing applications compared to the amounts on offer through the grant process. Questions were raised about the medium term, such as about what Defence would do with the immediate result of collaborative efforts. Some noted that it's difficult to make investment decisions for the medium term without any indication from government. The vision exists, but specifics ('You need to make R&D, finance and employment decisions') are, so far, short term.

On the specific programs introduced in the 2016 Defence Industry Policy Statement, firms were very complimentary about the work, the level of visibility and the information flowing from the Centre for Defence Industry Capability and their access to the centre's advisers. Comments on the Defence Innovation Hub were more mixed but, overall, firms observe that there's been a sea change in the attitude of Defence to working collaboratively with industry and in determining requirements since the establishment of the centre and hub.

As was picked up in the IIR, firms could readily see utility and benefit if the programs put in place in the Defence Industry Policy Statement were separately put in place in the intelligence and security domains. More generally, respondents (who had exposure to the defence domain) highlighted the lack of information covering the intelligence and security domains.

Respondents reported that the vast majority of R&D work was being undertaken for the defence domain. While this reflects market size, it was noted that in the intelligence and security domains little information about R&D needs was available. Without clearly set out requirements, it's difficult to engage meaningfully on future needs. Across all areas, there's still very limited engagement in formulating and refining R&D requirements or defining precisely what's to be sourced from the private sector.

Some respondents hoped that, in the intelligence and security domains, the present lack of an R&D strategy available to industry might be rectified as the Home Affairs portfolio matures. Many reported that programs such as the Next Generation Technology Fund and the Small Business Innovation Research for Defence program are good initiatives and that similar initiatives are required for the broader national security community.

A research entity noted that R&D isn't an off-the-shelf product, so it obviously doesn't fit the usual government request for tender approach and rules. Collaboration sounds good to government until researchers in industry and universities start talking about unknown outcomes and unpredictable discovery.

Overall decline in R&D investment

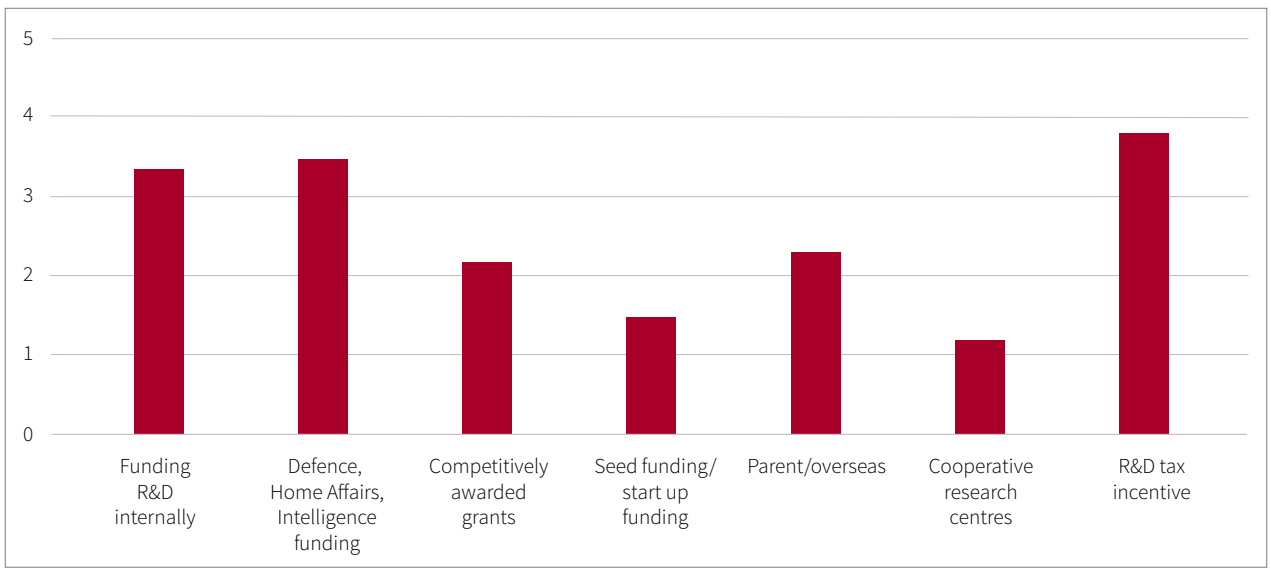
A diverse range of reasons was offered to account for the overall decline in Australian business R&D investment over the past decade, as shown in ABS data. Some respondents noted R&D funding increases. Others, from small to medium-sized enterprises, noted poor engagement with R&D providers. Both these points are supported by the 2017 *Australian innovation system report*, which noted that the decline since 2009 appears to have been driven by large reductions in mining and manufacturing R&D expenditures and that the business sector as a whole is not particularly well connected to the research sector.[54]

Respondents noted a lack of a whole-of-government approach to R&D capability development, the limiting effect of government preference for the least risk, and precertification or standardisation requirements that reduce incentives to invest in R&D, as it would produce novel results.

In the Defence portfolio, priority attention has been given to 'big ticket', typically foreign, procurement, at the expense of local R&D investment. Respondents thought the prevailing culture was that risk trumps innovation, although in recent years that attitude appeared to be starting to change. Similarly, one rationale offered was the perception that opportunity costs appeared to be too high.

The R&D tax concession was identified as the most important instrument for funding R&D among firm respondents, followed by funding from Defence, Home Affairs and the intelligence community and internal R&D funding (Figure 6).

Figure 6: Sources of R&D funding, rated by importance



Firms were particularly critical of changes that have taken place to the R&D tax concession over the past decade. Several said it has grown harder to claim, and that the eligibility criteria and oversight have been constantly tightening. Business is thus partly incentivised to fit R&D to changing tax criteria rather than to focus on R&D challenges. External expert tax advisers are increasingly required to assist with paperwork and new regulations, which adds cost and additional risk.

While the Treasury has been undertaking consultations to further consider the R&D tax incentive amendments announced in the 2018 Budget,[55] the sector was nearly universally concerned about adverse implications, although views about individual aspects and impacts varied, given their wide-ranging R&D activities and the size of those activities. In addition to favourable bottom-line impacts for R&D resources, respondents noted that special consideration for national security was warranted for specialised (unique for single or very few customers) software development and that R&D investment write-offs (given the small market and high failure rates of projects, tenders and start-ups) would be an innovation stimulus.

Start-ups noted that R&D tax incentives were problematic, given their unique cash flow model (for example, quarterly payments would be helpful) and that the $4 million cap on refunds for companies with turnover under $20 million (announced in the 2018 Budget) was restrictive and regrettable. It was noted that the Budget announcement included an exemption for clinical medical trials, given the need to 'develop life changing drugs and devices'. The need for competitive national security should also be considered reason enough for the same exemption. Secrecy was also noted as a complication in accessing the current R&D tax scheme, as it obliges firms to weigh up measures for protecting intellectual property against engagement requirements. A subcategory in the tax scheme to accommodate the special circumstances of national security start-up enterprises, along the lines of that proposed for medical research, was suggested.

Communications

Respondents widely noted recent significant improvement in government communications, particularly about defence innovation. However, they were critical of communications about R&D priorities, which they described as top level, passive and general. The onus is then put on firms to respond, but at lower levels, with active and specific proposals. This disconnect between government on one side and industry–academia on the other often requires firms to find or cultivate a champion within Defence. Respondents noted that, while agencies and officers are naturally cautious about exposing capability gaps, it isn't very efficient to flag general fields and then hope someone responds with an answer to the specific problem. The better defined the requirement or challenge statement is in the first place (although subject to ongoing refinement), the better the chance that R&D will stay on track to deliver a solution.

Participants noted that there's limited penetration of priorities within the R&D ecosystem outside Defence because the priorities are too generally defined. Seasoned respondents noted the importance of building trusted relationships in order to understand where real needs exist. Newer respondents noted that the pace of technological development and the nature of contemporary business models mean that a trusted relationship that might take 10 years to develop is an unfeasible prerequisite for innovation in 2018.

There's limited cross-agency management of linkages and opportunities, making it too hard for external providers to navigate. There appears to be a disconnect between the language used by the defence, intelligence and security sectors to describe their needs and the language needed to describe the types of technical expertise they are seeking from the R&D sector.

Start-ups

The response rate from start-ups was modest. Most companies contacted said that policy questions were not a (time) priority in a subsector in which company survival is less than 10%. Respondents did report support for the government's 2015 National Innovation and Science Agenda and the 2016 Defence Industry Policy Statement, particularly the Next Generation Technology Fund and the Defence Innovation Hub. It was noted that the recent consolidation of innovation programs within Defence made things simpler, but that agility and the capacity of government staff, whatever their organisational arrangements might be, are more important.

Common points included the need for government to appreciate the pivotal importance of execution speed. Start-ups operate on a live-or-die succession of short-term finance arrangements. This reality requires decisions and payments to occur within periods of several weeks to a few months, whereas an established revenue-generating company can accommodate government decision-making on a timescale of several months to a few years.

Uncertainty was a particular issue for start-ups. Uncertainty about the timing of future rounds, payments and announcements is in itself a deal breaker. If an official says 'they reckon' or 'it should happen' by a certain date, that's not good enough—you can't trade while insolvent and you can't invest based on heavily caveated best guesses of junior officials. Frequent (annual) policy changes also increase uncertainty.

Finally, start-ups identified a need for a formal avenue though which unsolicited proposals (covering a wide range of technological readiness levels) pursuant to general national security R&D interests would be useful and motivational.

While responses from the start-up sector were too small to be taken as representative, the comments were nevertheless consistent with start-up sector submissions to the government's 2016 review of the R&D tax incentive scheme.[56]

Policy ideas

Respondents submitted and discussed a range of policy suggestions for improving the take-up of R&D by Defence, Home Affairs and the intelligence agencies over the next five years:

- Develop a clear and more detailed statement of whole-of-government national security R&D requirements and challenges over the short, medium and long terms.
- Develop a facility to enable cross-departmental linkages.
- Allow research entities to interrogate national security agencies 'in confidence' to better understand the agencies' needs.
- Government could sponsor appropriately classified liaison experts to share understandings and develop challenge – challenge-solver registers to join up government, academia and industry to tackle problems.
- Establish a whole-of-government national security capability fund.
- Speed up engagement turnaround times—set targets.
- Establish a national security cooperative research centre.
- Commit to development pathways (including divestment of R&D to date if the capability priorities change) upon successful stages of R&D.
- Establish a dedicated testing area for unmanned vehicles (including for autonomous underwater vehicles).
- An increased focus on equipping the ADF with Australian-developed technology would stimulate greater investment.

Case study: Silentium Defence

In 2007, Dr James Palmer and Simon Palumbo initiated research on passive radar technology at the DSTO. After more than a decade of R&D and maturing the technology inside Defence, Silentium Defence was incorporated in 2016 to commercialise the technology and to transition it from prototype to capability. Passive radar can provide broad-area situational awareness in the same way that traditional radar does but without creating an active radio frequency signature. Instead of transmitting, passive radars exploit pre-existing sources of electromagnetic energy (such as broadcast television, radio, and so on) as their donor signal source.

Silentium Defence is unique in that it's the first spin-off from Defence in decades and a deep-tech start-up with both defence and civilian applications. While maintaining a small radio frequency signature is a significant advantage for Defence, not having to pay for spectrum licences and not creating any electromagnetic radiation hazard provide benefits to both Defence and civilian customers.

The world-leading capability that Silentium Defence is developing has attracted development support from government (SA Early Commercialisation Fund through TechInSA), civilian customers (Boeing Phantom Works) and Defence innovation-funding mechanisms (the Defence Innovation Hub). A critical start-up function is the ability to 'fail fast, fail-cheap'. This requires rapid feedback from the target customer segment in order to readily adapt the value proposition of products and services according to market need. To use start-ups and their innovative methods, early interoperability needs to be established between government and start-ups. Rapid decision-making (several weeks to a few months rather than several months to a few years) is the pressing challenge for large government departments.

Policy options that can drive rapid engagement and enable fail-fast, fail-cheap iteration include non-dilutive investment programs for start-ups, such as the US Defense Innovation Unit (dubbed the 'Pentagon tech office in Silicon Valley', the unit is a fast enabler of emerging commercial technology). Another option is to formalise mechanisms to transition intellectual capital from government and independent research entities into start-ups, pursuant to the creation of national security capability. Another option is the explicit and regular communication of whole-of-government national security R&D needs and interests to the start-up sector.

NATIONAL SECURITY R&D

Australia's national security R&D investment has not maintained a proportional share of Australia's gross R&D expenditure. Since 2000, government defence R&D expenditure has flatlined in real terms and declined relative to both the defence budget and the national research budget. Over the same period, Australia's private defence R&D expenditure has declined in both real and relative terms.

Despite recent policy adjustments that have improved government defence collaboration with academia and industry, government and private expenditure are static at best and remain focused on procurement and support for military platforms and ADF operations. While addressing procurement and operational needs (with due emphasis on the cyber domain), our defence and national security apparatus, in its scale and focus, has under-responded to global technological progress.

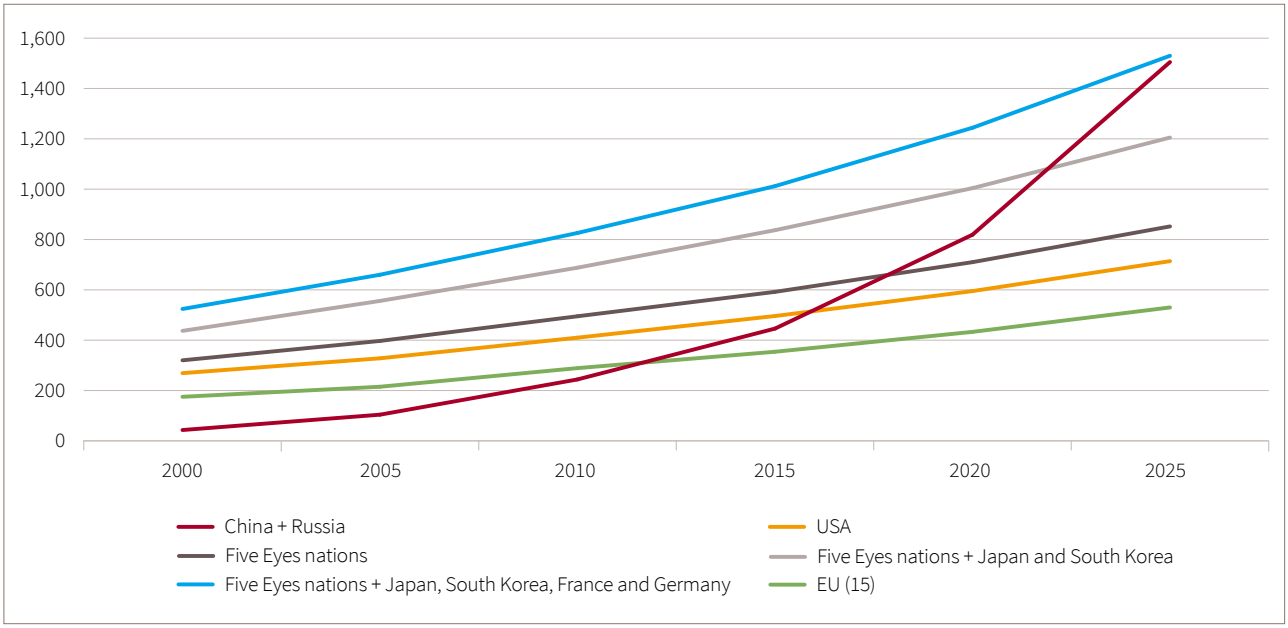
Orthodoxies

Orthodox defence technology theory holds that the technology contest, while central, is nevertheless subservient to the contest to strategically deploy new technology. This is because ready proliferation is assumed: what one side deploys, the other side can very soon counter. This theory is well grounded, but the assumptions that proliferation is visible and that our ability to readily and thoroughly respond remains constant depend on conditions that are now changing. The scale and location of R&D growth underway worldwide, and the speed of technological development, undermine both those assumptions. Free market drivers are overtaking (known) government (geopolitical) drivers of most global R&D, which further weakens the theory's validity. Lastly, as the unpredictability of technological development remains constant, and as sources of innovation diversify, so too do the origins of surprise innovation.

Sustainable advantage

It's tempting to consider the dominance of OECD R&D to be unchallengeable. Although it's well noted that our general R&D advantage and defence technology advantage are in decline,[57] OECD nations clearly lead virtually all technology fields and subfields. However, basic projections of global R&D expenditure growth suggest that investment parity, at least, isn't far away. Investment trends since 2000 suggest that authoritarian nations, led by China, are set to match Five Eyes investment by 2020. By 2025, if average growth rates since 2000 continue, those countries will match Five Eyes investment plus the investments of Japan, South Korea, France and Germany (Figure 7).[58] Gross R&D expenditure paths of a dozen countries are not likely to follow a static projection, but the possibility of some normal variation of this scenario needs to be seriously considered.

Figure 7: Gross national R&D expenditure, selected groups, 2000 to 2025 (US $billions PPP)



Source: OECD, 'Main science and technology indicators', *OECD.Stat*, online.

In addition to our declining relative expenditure advantage, there are structural reasons why special consideration must be given to defence and security R&D. The first is that such efforts focus national resources to tackle particular threats and opportunities. This affords 'critical mass' investment in challenges pivotal to national security interests. This expenditure is a very minor percentage of total national R&D expenditure: a minimum critical mass is well within the budget of the largest 15 nations by GDP. For example, Japan, South Korea and China have recently established DARPA-like functions to focus their national R&D strengths on high-opportunity national security needs and opportunities.[59] In 2018, Germany announced plans to establish a DARPA-like agency with an expected focus on cybersecurity, artificial intelligence and improved engagement with start-ups.[60]

The second reason is that modern research tools and methods and the availability of knowledge and data enable more productive R&D (that is, less time and resources per output). For example, North Korea was able to develop and demonstrate intercontinental ballistic missile and nuclear weapon technology faster than was generally predicted. North Korean defence R&D personnel were tackling known, and known to be solvable, challenges, but, importantly, they were doing so with contemporary research tools. There's no doubt that established technology owners provided some assistance, but the speed of the North Koreans' progress was probably due in part to the use of general-purpose (high-end) computers and modelling software. This provided a short cut compared to time-consuming physical experimentation.

Research equipment that was state of the art five years ago but that has become redundant (due to lower speed and specificity) and greatly depreciated (measured by the cost of scrapping it) is increasingly being recycled and repurposed.[61] Global research output is also producing and making available vast datasets in every field. Modern general research tools and methods will universally hasten the development and proliferation of known defence technologies, as well as new technological disruptions relevant to national security.

Finally, and potentially of transformative impact, is that artificial intelligence (AI) applications will help overcome S&T knowledge and capacity deficits. In particular, AI-aided interpretation of global R&D product will allow R&D investment to be applied with the benefit of all available current knowledge. Traditionally, experienced specialists provided such knowledge, having accumulated it over decades of cutting-edge R&D. The average researcher reviews 270 articles per year, and senior researchers and developers have professional life knowledge of several thousand papers. With about 3 million articles now published annually, up from 1 million in 2000,[62] even highly specialised

in-field experts struggle to be sure of contemporary worldwide understanding. Deep learning algorithms can scan and maintain contemporary awareness of the world's 50 million+ published R&D works to assist researchers to stay abreast of the sum of knowledge on particular topics.[63]

Beyond ensuring that R&D efforts build upon state-of-the-art understanding and avoiding the duplication of work, AI and simulation technology (dynamic models) will also aid research to hasten results and improve quality. Machine-learning algorithms can boost the power and speed of data analytics, exploiting learned expertise to quickly raise research capability from beginner to advanced levels. Such assistance to make the most of global research outputs and undertake R&D stands to revolutionise the capacity of research groups to tackle unfamiliar topics from a standing start. Australia can and should invest in these R&D tools and technologies.

This emerging ability will be especially useful in fields that depend upon multidisciplinary research or present as a surprise and require a rapid response. Just as situational awareness is a primary objective of defence and security policy, it's equally important to S&T progress. The complexity of multidomain battlespaces and the speed with which events can potentially unfold place even greater emphasis upon technological preparedness.

Fields of disruption

Many technological fields are recognised as being directly relevant to national security. The scientific and tactical merits of those fields are well explored elsewhere. The following sections consider policy on current, relative and potential Australian engagement in four selected fields.

Artificial intelligence and machine learning

In March 2018, France committed €1.5 billion to boost AI R&D over the next four years.[64] President Macron noted that 'There's no chance of controlling any effects [of these technologies] or having a say on any adverse effect if we've missed the start of the war …' Policy objectives include mitigating France's AI and ICT brain drain, leveraging ethical advantage opportunities and catching up with US and Chinese tech giants.[65] The stated sectoral applications of France's AI policy are defence and security, transport, the environment, and health.[66] More broadly, the EU has announced an expansion of investment in AI and is aiming for total private and public investment in the field to reach A$24.36 billion by 2020.

By comparison, Australia's 2018 Budget committed $29.9 million to boost our modest AI R&D investment over the next four years. Reflecting Australia's sectoral focuses, funding has been split between the Department of Industry, Innovation and Science, CSIRO and the Department of Education and Training.

In November 2017, the UK Government unveiled its strategy for positioning the UK to become a world-beating, wealth-creating economy. Aside from funding three new university-based supercomputers to support research, it set aside funds to provide grants for 450 PhD students and a further A$50 million for digital courses using AI as part of a larger retraining effort for the British workforce. In addition, the UK has set up the National Advisory Body for AI; the body is linked to its Centre for Data Ethics, which develops standards on the use and ethics of AI and data.

Canada's AI strategy aims to attract tech talent from offshore via a fast-track visa linked to permanent residency. Acknowledging the acute shortage of AI talent globally, the Canadian Government has set aside A$130 million to establish research labs linked to universities in Toronto, Montreal, Edmonton and Waterloo.

Japan's fiscal 2018 budget has allocated A$860 million to AI-related activity. The bulk of it is linked to robotic research, medical data management, next-generation AI computer chips and pharmaceutical technology.

In a national video broadcast to schools in 2017, Russian President Vladimir Putin said:

> Artificial intelligence is the future, not only for Russia, but for all humankind. It comes with colossal opportunities, but also threats that are difficult to predict. Whoever becomes the leader in this sphere will become the ruler of the world.[67]

As rhetoric, it sent a clear message about the relevance of AI, which is further supported by calls to combine military and civilian R&D efforts.[68]

In December 2017, Google revealed that it would establish an AI research centre in Beijing, with several hundred staff, in order to access talent, data and markets.[69] At the 19th meeting of China's National Congress in 2017, President Xi Jinping confirmed that AI, big data and the internet are the three fields that he's looking at to build the country's strategic and economic strength. His statement to the Congress confirmed decisions taken by the State Council in mid-2017 to allocate A$190 billion to position China as an AI innovation centre by 2030.

In January 2018, the Vice President for Research at Massachusetts Institute of Technology (MIT) noted that, over the next five years, the Chinese Government plans to invest 100 times more in AI than the US Government did in 2016.[70] This is consistent with China's stated ambition to 'become the world's premier artificial intelligence innovation center' by 2030 in order to 'foster a new national leadership and establish the key fundamentals for an economic great power'.[71] In January 2018, China announced that it would establish a US$2.1 billion AI industrial park—its first major investment towards the 2030 target.[72]

Of world research entities with the most cited AI-related research papers from 2012 to 2016, China has two in the top 10, while the rest are in the US (5), France (1), Canada (1) and Singapore (1). Asian nations had 25 in the top 100, of which Australia hosts 4 (the University of Technology, Sydney; the Australian National University; the University of NSW; National ICT Australia Ltd[73]), China has 14, Singapore has 3 and Hong Kong has 3.[74]

A 2017 report by the Belfer Center for Science and International Affairs at Harvard Kennedy School, on behalf of the US Intelligence Advanced Research Projects Activity (I-ARPA), titled *Artificial intelligence and national security,* noted that:

> AI has the potential to be a transformative national security technology, on a par with nuclear weapons, aircraft and computers. Each of these technologies led to significant changes in the strategy, organization, priorities, and allocated resources of the US national security community … [F]uture progress in AI will be at least equally impactful.[75]

In June 2018, the US Department of Defense delivered its Artificial Intelligence Strategy to Congress. An unclassified version of the report hasn't yet been published, but a department spokesperson said:

> The AI Strategy emphasises the need to increase the speed and agility with which we deliver AI-enabled capabilities and adapt our way of working, the importance of evolving our partnerships with industry and academia, and the Department's commitment to lead in military ethics and AI safety.[76]

Australia's expenditure stands in stark contrast to decisions taken by governments of our major trading partners, which accept that AI, as a technology of significant national importance, has passed a major inflexion point. Australia's defence and national security would benefit from a coherent national AI strategy that enables a critical mass of R&D investment and from an adequate budget to implement competitive AI technologies.

As Australia's Chief of Army noted in August 2018:

> While the nature of war as a contest of wills is enduring, technological disruption is rapidly changing war's character. These characteristics include the convergence of big data, artificial intelligence, machine-learning, robotics, unmanned and autonomous capability with precision weaponry.[77]

Medical science and technology

Medical and health research is Australia's broadest, world-leading research field. This reflects our general research excellence and recent investment profile in the field. In 2016, $5.9 billion was spent by all Australian sectors on health and medical research.[78] The federal government's commitment via the National Health and Medical Research Council (NHMRC) grew from $150 million in 2000 to $829 million in 2018.[79] Additionally, the Medical Research Future Fund, established in 2014, has started to deliver returns and is set to reach its $20 billion capital target in 2020.[80] Support for national security objectives in this field is not currently an Australian priority.

Just over 100 years ago, a strain of H1N1 influenza emerged and killed at least 50 million people out of a worldwide population of around 2 billion.[81] Its spread was enabled by mass transport systems. Today's world population of 7.6 billion is many times denser, interactive with animals and interconnected physically and temporally. Viruses naturally evolve and move between species as opportunity allows. New viral varieties and other pathogens won't necessarily remain stable; nor will outbreaks necessarily be manageable.

Pandemics are a high-impact, low-risk threat. Hence, maintaining biosecurity is a daily challenge to our border protection agencies, which also seek to maintain the integrity of our food and fibre industries and Australia's general biodiversity. Despite modern medicine, veterinary science and biosafety technology, these risks can increase, mostly driven by factors external to Australia: population growth and globalisation. Convenience and cost drivers cause medicine and health technologies to proliferate, which increases the prospect of both new solutions and new threats.

Pandemic mitigation also depends on the integrity and resilience of the supply chains that provide drugs, materials and services. Evolving antibiotic resistance presents challenges to the supply of effective drugs, and diseases such as typhoid are becoming increasingly resistant.[82] The World Health Organization warns that:

> [T]he world is headed for a 'post-antibiotic era' in which common infections and minor injuries which have been treatable for decades can once again kill, and the benefits of advanced medical treatments such as chemotherapy and major surgery will be lost.[83]

Resistance to antimicrobial and antiviral drugs demands competitive innovation in their deployment and development to stay ahead of evolutionary forces.

This challenge to the efficacy of current treatments is also a security challenge, because today's easily treatable pathogens may be put to malicious use according to the effectiveness of available medicines. The development of new types and classes of antibiotics is a major R&D objective worldwide. While Australia is a small but significant contributor to that effort, national security related R&D in this field is minimal and coincidental.

In 2000, bioengineering (synthetic biology) was restricted to advanced research laboratories, but it's now a proliferating technology. Gene editing is now a relatively affordable retail service, and equipment to produce genetic modification products will soon become as easy to use and afford. Human genomes can now be sequenced at a small fraction of the cost of a decade ago, and this is now a genealogy quasi-novelty service. Gene drives (precision addition, subtraction or modification of the genome) enable the breeding of a particular suite of genes within a population. Genomic understanding, rather than the availability of effective tools (such as CRISPR-Cas9 enzymes), limits the potential utility of this technology. Dual-use issues abound, as the ability to delete hereditary disease also provides the means to add certain qualities. The development of 'super traits' will challenge social and ethical norms, provide particular advantages (pathogen resistance) and, for humans especially, have the potential to affect future generations because editing can alter human inheritance.[84]

All these cases have growing security implications for an island nation that trades upon the quality of its biosecurity. Fortunately, due to substantial growth in health and medical research, Australia has the knowledge creation ability to address these threats. The US has such mechanisms. In addition to DARPA, the Biomedical Advanced Research and Development Authority (BARDA; budget ~US$500 million p.a.) manages R&D for countermeasures against

bioterrorism, as well as against pandemic influenza, emerging diseases and chemical, nuclear and radiological threats. The US Defense Department's Congressionally Directed Medical Research Programs fund (~US$1 billion p.a.) high-impact, high-risk collaborative R&D for service personnel, veterans and the public. International collaborators include Australia (for example, in work on traumatic brain injury and post-traumatic stress disorder).

Case study: Virology at QUT for DARPA

Since 2017, DARPA has funded a collaborative effort, led by the Queensland University of Technology (QUT) Arbovirus Group, and including Duke–National University of Singapore Medical School, the Queensland Institute of Medical Research and the QUT Modelling Group, to develop novel and adaptive therapeutic countermeasures to prevent or treat dengue infection. This is part of the global DARPA INTERfering and Co-Evolving Prevention and Therapy (INTERCEPT) program, which aims to deliver new therapeutics for fast-evolving viruses such as influenza, Zika, Ebola, dengue and Chikungunya.

Many viruses with RNA genomes are known to generate defective virions during replication, and those defective particles can reduce the amount of infectious virus produced in subsequent cycles of infection. The Arbovirus Group at QUT has observed this during dengue virus infection and shown defective dengue virions to be transmitted in nature for several years. DARPA has provided $2.5 million over two years for the Australian team to develop a system to produce sufficient quantities of defined defective dengue virions, under good manufacturing practice, to be able to undertake trials in experimental animals and, if those trials are successful, in humans.

An Australian source of funding for such work would provide three benefits. First, it would ensure that Australia is able to build upon and take advantage of R&D progress in a timely manner. Second, a national security grant scheme would ensure reliable, ongoing priority for relevant health and medical science R&D. In doing so, it would improve Australian security preparedness and contribute to allied R&D investment in recognised fields of importance while advancing broader human wellbeing. Third, such a strategic commitment would significantly enhance Australia's security capability through the development of talent, know-how, intellectual property, knock-on and spinoff opportunities.

Given the UK's current experience with the nerve agent Novichok, and the proliferation of technologies to manufacture sophisticated compounds, Australia could develop defence capabilities to such emerging threats with innate strength.

Social and behavioural science

Australia's social science research base is also excellent. While defence R&D traditionally focuses on platforms and hardware (and recently on cyber capabilities), social science fields cover the changing dynamics of Australian society and ICT-driven global interactions, which are most relevant to intelligence and domestic security agencies. The fusion of physical sciences and social sciences is shaping global society. For example, the world's biggest ICT company by revenue, Apple, isn't a microprocessor or network maker but a product and service provider that has created enormous public value through both technological and sociological understanding.

The fields most affected in Australia by ICT innovation over the past 30 years are studies of human society; psychology and cognitive sciences; ethics; law and legal studies; language and communication; culture; and history. The R&D skills of anthropologists and sociologists are needed in the current and future national security R&D space and yet they're only very modestly represented in our current workforce.

Australia's current national security investment in these fields is so modest that public investment per annum isn't explicitly measured. Guarding social identity and the integrity of our democratic institutions and processes requires strategic R&D at a meaningful level in fields such as cultural studies, social media and cognitive behaviour. Efforts to counter (deter, detect, mitigate) weaponised narratives, for instance, will require cutting-edge social and behavioural science resources just as much as the physical science capabilities that underpin ICT.

In 2016, the US National Academies of Sciences, Engineering, and Medicine began a three-year survey of the social and behavioural sciences to understand how emerging knowledge may be directed and applied to assist the work of the US national security community.[85] Given our shared interests and Australia's research strengths, the forthcoming report of the Social and Behavioral Sciences for National Security project, due to be published in early 2019, will offer useful guidance for Australia about collaborative R&D investment decisions and applications over the next decade.

As scientific understanding expands, traditional discipline boundaries blur; for example, nanotechnology combines physics, chemistry, biology and mathematics at the molecular scale. Innovative technological advances commonly occur between the boundaries of traditional fields of understanding. The 'brain–computer interface' is such a subject, with profound potential for disruption, combining neurological and physical sciences and, presumably in the future, psychological sciences. The best known neuroprosthetic device is the Cochlear implant, which overcomes profound sensorineural hearing loss. Cochlear Limited, founded in Australia the early 1980s in partnership with the Australian Government, undertook the R&D and pioneered the product.[86] Potential products and services based on brain–computer interface technology are easy to imagine, as are potential security concerns arising from them (see box).

Case study: Direct neural interface

In 2018, MIT researchers announced the development of a computer interface that can transcribe words that the user mentally verbalises but does not speak aloud.[87] The system consists of a wearable device that rests along the jawline from ear to chin. Electrodes in the device pick up neuromuscular signals triggered by internal verbalisations (saying words 'in your head') but that are undetectable by the human ear or eye. The signals are fed to a machine-learning system that trains to correlate particular signals with particular words. This computer interface with internal verbalisation is just one type of machine–human interface advance.

Commercial and public R&D into direct neural interfaces (brain–mind–computer–machine) for communication, the control of virtual and real tools, cognitive monitoring and general R&D purposes is driving a commercial market that's growing at a compound annual rate of 17.6% and are expected to be worth an estimated $1.8 billion by 2023.[88] Applications range from health, robotics, education and safety to defence and security. Australia has three research groups working in the field and has produced commercial spinoffs in the past.

In the 2000s, an Australian start-up, Emotiv, was founded to commercialise an innovative Australian university born electroencephalography (EEG) interface. This was one of the first mobile EEG devices available to the market. Emotiv is now a market-leading medium-size private company based in San Francisco, California.[89]

Supercomputers

As research tools to provide the best quality modelling services (such as meteorological forecasts), supercomputers are key elements of national R&D infrastructure. In 2018, Australia had five supercomputers in the world's top 500, as rated by processing power.[90] Two are research machines, one of which is at the National Computational Infrastructure National Facility based at ANU (ranked 102, down from 70 in 2017) and the other of which is at the Pawsey Supercomputing Centre in Western Australia (ranked 217). The three others are private cloud service providers (ranked 105, 200 and 386).

While smaller economies than Australia feature in the top 100 (Sweden, Switzerland, Spain and Saudi Arabia), Australian researchers' access to supercompters (per hour as needed) has improved relatively due to global proliferation in the number and performance of rentable machines in recent years. The 2018 Budget included a provision of $140 million to upgrade the research supercomputers, which ought to maintain their relative performance over the short term.

By comparison, the US Government and US industry had 32 in the top 100 and 124 in the top 500. China (government and industry) had 23 of the top 100 and 206 of the top 500.[91] Importantly, the private sector operates more than half of the top 500.

Australia's comparatively modest supercomputing facilities are not world leading, but global access to processing services works for most research. However, storing data that has national security sensitivities, or running programs or algorithms that use it to produce sensitive results, requires a secure domestic environment. Experimentation, research and training, and running models or machine learning applications pursuant to national security functions, typically use both sensitive software and data for which secure domestic supercomputing facilities are required.

R&D ecosystem needs

> New commercial technology will change society and, ultimately, the character of war … Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base.
>
> —Summary of the 2018 *National Defense Strategy of the United States of America*, January 2018, online.

To provide innovative technological solutions and services, the national security R&D ecosystem needs to be supported as a whole. Key elements needed to underpin a productive and resilient system that accommodates necessary risks, and that state and federal governments may facilitate, include infrastructure, capital, human resources and collaborative mechanisms.

Government infrastructure

The Australian Government's 2018 response to the 2016 National Research Infrastructure Roadmap and Research Infrastructure Investment Plan set out a strategic, whole-of-government view.[92] However, the consolidated approach to understanding national research infrastructure needs did not produce a road map with focus areas that include defence or national security areas.[93] The primary recommendation agreed and funded in the 2018 Budget was:

> Recommendation 1. Adopt nine focus areas and their priorities to strengthen our economy, advance societal benefit, improve our competitiveness, and build on our existing national capability. These focus areas complement the National Science and Research Priorities and the Industry Growth Centres [Initiative].

Apart from cybersecurity, national security R&D is not one of the national science and research priorities or one of the six 'strategic priority' industry growth centres.[94] The medium- to long-term infrastructure needs of the national security R&D sector should be identified and incorporated into Australia's overall research infrastructure planning and included in the National Collaborative Research Infrastructure Strategy. The separation of national security R&D policy from general government R&D policy hinders collaboration, constructive planning and strategic national progress.

National security R&D infrastructure needs that should be considered for future investment include supercomputers; software and data management infrastructure; test facilities; hazardous material laboratories; electronically secure workplaces; space industry; manufacturing infrastructure; and training and personnel development infrastructure. Capacities and equipment currently operated by the national security R&D sector, primarily Defence, might similarly be further supported and used by the broader Australian R&D community as collaboration develops.

Capital

The availability of research funding and venture capital for particular fields limits the extent of R&D activity and the risk–reward profiles of projects.

The government's nine science and research priorities are food; soil and water; transport; cybersecurity; energy; resources; advanced manufacturing; environmental change; and health.[95] Funding to pursue these areas is primarily delivered by the Australia Research Council (ARC, budget ~$750 million p.a.) on a competitive basis using grants for career stages, industry linkages, industry transformation, basic discovery and centres of excellence. Federal and state government departments fund R&D according to portfolio directives. The NHMRC (budget ~$830 million p.a.) funds health research according to national health priority areas, which are dementia; obesity; arthritis and musculoskeletal conditions; asthma; diabetes mellitus; mental health; injury prevention and control; cardiovascular health; and cancer control.[96] Additionally, the government wisely established the Medical Research Future Fund, which is budgeted to reach its capital target of $20 billion by 2020–21; the interest it generates will fund strategic medical research.

R&D applicable to national security can and does fit into the listed areas, but has been given no such priority. Research funding is highly competitive. The average research proposal success rate is around 15% and falling, and there's open acknowledgement that the quality of proposals is improving against stagnating resource levels.

Until the 'Safeguarding Australia' national research priority was dropped in 2013, five R&D goals concerned national security: critical infrastructure; understanding our region and the world; protecting Australia from invasive diseases and pests; protecting Australia from terrorism and crime; and transformational defence technologies.

Australia's venture capital market has grown off a small base (~$350 million in 2013) to about $700 million p.a. in 2018. In the first quarter of 2018, it reached $130.5 million, raised from 16 transactions. By comparison, in the same quarter, the US raised US$29.4 billion from 1,782 deals, Asia raised US$14.6 billion from 317 deals, and Europe raised US$5.2 billion from 548 deals.[97] Australia's start-up strengths are in business-to-business services and financial, agricultural, design, education and construction services.

Investment since the launch of the Defence Innovation Hub in December 2016 (purportedly $64 million p.a. over a decade) and the Next Generation Technology Fund in March 2017 (purportedly $73 million p.a. over a decade) is unclear. While legacy (pre-2016) innovation projects worth approximately $61.2 million were transitioned into the Defence Innovation Hub,[98] program-level financial year expenditure hasn't been reported. Ministerial media releases suggest that resources additional to previous annual averages for R&D will be committed, but annual budget details so far are presumably too small to warrant inclusion in the annual report.[99]

There have been encouraging new R&D initiatives. In June 2018, as a result of the 2017 Army Innovation Day's 'special notice' call for proposals in response to specific capability challenges, the Defence Innovation Hub awarded contracts ($2.2 million) to explore the ADF's desired capabilities.[100] One example is the Defence Materials Technology Centre (DMTC) and its leadership of a national Medical Countermeasures R&D program that's designed to deliver enhanced national health security capabilities.[101] Having attracted $5 million initially from CSIRO and then a further $5 million from Defence under the Next Generation Technologies Fund, industrial and research partners have also co-invested in the program. To date seven R&D projects have been launched involving 17 industry and research partners, each of them undertaken by an industry-led consortium. A recent solicitation for a third round is expected to add another three or four projects to the program.

DMTC has continued to make an important contribution to Defence innovation and provided support for the Defence Innovation Hub through its unique capabilities and networks. The Innovation Hub's investment through DMTC (set at $3 million per year in the 2016 Defence Industry Policy Statement) attracted an additional $20 million in co-investment from industrial and research sector partners and Defence program offices in FY2017-18. This enabled

a range of collaborative technology development activities to occur, aligned with the Hub and DMTC's shared goal of enhancing Defence capability through innovation. DMTC's partnership with the Next Generation Technologies Fund on Medical Countermeasures research and product development is a demonstration of the single innovation pipeline described in the 2016 Defence Industry Policy Statement.

In May 2018, four Australian universities joined with US universities under the US Department of Defense Multidisciplinary University Research Initiative to work on material and quantum science projects.[102] The government provides financial support for Australian universities to engage with it via the Next Generation Technology Fund ($25 million over nine years).[103] The 2019 topic for Australian projects under the initiative is 'Active perception and knowledge exploitation in navigation and spatial awareness'. The sum of $2.7 million p.a. is about the right critical mass for one collaborative research project, but the most encouraging aspect is the appropriateness of the time commitment. The medium- to long-term collaborative approach is sensible, but the scale appears, at best, to be only slightly improved.

The UK sets a useful example to consider, particularly in its identification of the function of 'patient' capital in the innovation ecosystem.[104] The UK Government's response to a 2017 UK Treasury consultation, *Financing growth in innovative firms*,[105] which included a UK Treasury review of patient capital,[106] was in the form of 2018 budget measures to help finance growth in innovative firms. Primarily, a new £2.5 billion investment fund was established to leverage a further £5 billion in private investment. National security innovation was an identified niche market that warranted the establishment of the National Security Strategic Investment Fund, with up to £85 million to invest in advanced technologies that contribute to the national security mission.[107]

The 2018 UK National Security Capability Review noted:

> In an environment where major threats are largely technologically driven, so too must be our response. The UK is in a strong position. Our scientific output is among the best in the world across the range of disciplines relevant to security. We must maximise this strength, particularly in emerging capabilities such as autonomy, robotics and data analytics. The UK Research and Innovation budget is increasing by £4.7 billion to 2020/21 and has wide-ranging potential national security benefits. The Government Chief Scientific Adviser will develop a new national security science and technology strategy through the NSC Officials' Science and Technology sub-committee.[108]

In September 2014, in recognition of geopolitical developments and technologically enabled challenges to the US's military-technological edge, then US Secretary of Defense Chuck Hagel launched the Defense Innovation Initiative. This formed the technological basis of the 'third offset' strategy/policy to mobilise innovation, new technologies and institutional reform in the pursuit of national security. From 2010 to 2015, US Department of Defense basic research grew by 12% and increased moderately as a share of the overall departmental budget.[109]

Under the third offset strategy, Defense Secretary Ash Carter expanded the Defense Department's long-time strategic engagement with academia (DARPA) to strategic engagement with the tech sector.[110] In 2015, he launched the Defense Innovation Unit Experimental (DIUx) to systematise the Pentagon's relationship with emerging tech companies in Silicon Valley, Boston and Austin. Starting with an initial budget of $30 million in 2016, the budget for the unit, which has since been renamed without 'experimental' as the Defense Innovation Unit (DIU) is $71 million for FY 2019, up from $41 million in 2018.[111]

Brendan Thomas-Noone has argued that, while the Trump administration's vocabulary has changed, the technological and institutional reform initiatives remain in place, and that Australia should seek to expand engagement with these initiatives.[112] The Trump administration and Congress increased DARPA's 2018 budget by 6.3% and for FY 2019 there's agreement (White House 12%, House 10.3% and Senate 12.2%) to increase it by ~12% to US$3.4 billion.[113]

Then US Defense Secretary Jim Mattis said of DIU in August 2017, 'I don't embrace it; I enthusiastically embrace it. And I'm grateful that Secretary Carter had the foresight to put something in place to anchor the Department of Defense out there'.[114]

Speaking at the launch of the US National Defense Strategy in January 2018, Mattis said:

> Our current bureaucratic processes are insufficiently responsive to the department's needs for new equipment. We will prioritize speed of delivery, continuous adaptation and frequent modular upgrades.[115]

Human resources

Human resources form the core of Australia's national security capability. As we argued in our 2015 Special Report, an ideal human resource model for the sector would provide reliable career scope within Australia's R&D community so that skills in demand for national security R&D could be readily available across government, industry and research entities.

Regrettably, little progress has been made in national security R&D workforce planning. The time taken to process security clearances, particularly for industry and non-government research personnel, appears to have increased.[116] Research, development and technology personnel are in high to very high demand from industry worldwide. Global industries and governments are buying innovation and research expertise (postgraduates, postdoctoral researchers, niche technicians and research leaders) with strategic forethought.

With the world's leading technology companies and start-ups undergoing rapid growth and offering lucrative sign-on bonuses and contract break compensation to secure staff, delays to secure security clearances further limit the talent pool available for both government and private national security related R&D. The demographic profile of cleared, qualified and experienced staff also presents a major challenge over the next decade, as retirement rates are set to exceed recruitment rates.

Just as global competition for high-quality tech staff has increased,[117] talent is noted to be the single biggest challenge facing Australian start-ups.[118] As mentioned above, while the competition for talent is growing, staff numbers at DSTG have dropped by almost 300 since 2013–14.[119] Anecdotally, the number of unfilled S&T positions across both the government and the private sectors is increasing.

To turn the situation around, a strategic plan for national security R&D personnel needs to be prepared to coordinate and guide sector development. The plan needs to cover both government and the private sector. Issues include qualifications, training, ongoing learning and career paths; workforce sustainability to ensure that future skills are available to meet future needs; gender and diversity measures to ensure the use of the best available personnel; and provision, maintenance and monitoring of security clearances that enable demand-driven movement between government, research and industries large and small, and those of allies and foreign suppliers.

Partnerships and international collaboration

Australia is rich in the most difficult-to-realise aspect of innovation: knowledge creation. To remain competitive as innovators, though, we need to vastly improve our ability to transfer and apply new knowledge. The most efficient way to realise these two practical capabilities, without diminishing our research capacity, is to invest in partnerships and collaborations. Nations whose weaknesses are in basic and applied research similarly invest in collaborative programs on this front. As discussed, efficient research practice is an open, multiparty endeavour, which necessarily limits the degree to which national controls can be applied. However, knowledge transfer and application are circumscribed endeavours, which may occur in defined (controllable) environments. The challenge for Australian national security R&D policymakers is to fill the basic research gap with open funding and to invest in the targeted, security-controlled development of game-changing technologies.

Naval Group: Australian Future Submarine R&D

In 2016, government selected majority French government-owned Naval Group to replace Australia's submarine fleet. The group's 2017 annual report details an R&D approach that's illustrative for Australia's national security R&D policy.[120]

'Naval Group spends around 2.4% of its revenue on self-funded R&D … This ratio equates to 9% if you include R&D contracts, subsidised R&D and R&D included in the programs.' Taking the Australian Future Submarine project (~$50 billion for procurement) as an example, the contract provides for ~$60 million p.a. over 20 years for self-funded R&D and ~$160 million p.a. for contracted, subsidised and program-specific R&D.

Under R&D activities, the report notes Australian Future Submarine R&D activity sold and to be retained: 'acceleration of work on the Australian Future Submarine program following Naval Group's retention by the client in April 2017 (R&D sold); in addition, work was done to retain our intellectual property in certain subjects.'

Australia doesn't possess, and therefore must buy, most high-technology military products. Naturally, suppliers seek to maintain their intellectual property advantage:

> The ability to manage Transfers of Technology (ToT) therefore continues to provide strong leverage for the group's international presence and the competitiveness of its product and service offerings; it is also a tool that allows our industrial processes to be turned to account for all our stakeholders, and ultimately the client that is France.
>
> The ToT process that has been set up, and is in force today, covers the entire draft proposal/offer/execution process. The extensive nature of these measures is very useful, especially during the proposal preparation phase; the benchmarking carried out has provided particularly valuable information.
>
> The current phase sees it being systematically rolled out to offers and programs, which will allow us to test, improve and standardise our ToT management processes as well as this tool kit. The Australian submarine program is emblematic of this roll-out.

So it should be noted that we're not only negotiating for existing intellectual property but co-investing in R&D over the long term, which prompts the question: how much of the result of ~$4 billion worth of Australian Future Submarine related R&D over the next 20 years will be accessible to Australia? Sensibly, Naval Group is also developing R&D road maps for both AI and unmanned maritime vehicles, in conjunction with French national research institutes.

In Australia, Naval Group signed a memorandum of understanding (2017) between Flinders University in South Australia and a consortium of four French engineering schools for Franco-Australian dialogue concerning student exchanges and collaborative research between academic and university structures.[121] As the submarine project is Australia's largest single R&D investment to date, ideally a reasonable proportion of innovative value and knock-on effects will be captured in Australia.

DISCUSSION

Overwhelming strategic advantage through innovation has long been the preserve of advanced nations. From firearms to gunboat diplomacy, deployable technological advantage was owned and operated by a global minority. In coming decades, thanks to the proliferation of data, science, technology, education and communication, new capabilities will be competitively developed and shared by a global majority.

How Australian national security arrangements adjust to this paradigm shift will partly shape our sovereign standing. A priority action of the 2017 US National Security Strategy was to understand worldwide S&T trends: 'To retain US advantages over our competitors, US Government agencies must improve their understanding of worldwide S&T trends and how they are likely to influence—or undermine—American strategies and programs.'[122] To protect our strategic interests, Australia should do likewise, focusing on our S&T strengths and weaknesses.

The Lowy Institute's 2018 'Regional Power' model ranks Singapore and Taiwan above Australia in technology as an element of economic resources.[123] This illustrates sound S&T policy outcomes of economies smaller than Australia's with far less research capacity. While the Lowy Institute's model considers economy-wide technology, the strengths identified for Taiwan and Singapore relate to national mission type R&D policies rather than, as the *Australia 2030: prosperity through innovation* report noted, Australia's 'heavy reliance on 'indirect' funding measures' (for example, our current ~$3 billion R&D tax arrangements).[124] Accordingly, the report suggested that Australia should 'increase the use of mission-directed support'. Mission-oriented R&D policy works by counterbalancing market restrictions, such as size, risk and opportunity costs, and limiting political and administrative uncertainty. This provides durable R&D conditions under which genuinely new capabilities can be developed.

As detailed above, collaborative R&D between Australian public research entities and the private sector is low compared to that in other OECD countries. The OECD's best performers characteristically have their industries take the lead on investment, weighted towards development, while their governments coordinate collaborative missions and take the lead on pure, basic and applied research. In contrast and with growing effectiveness, China's command-driven innovation policy obliges collaboration between the government and corporate sectors, taking advantage of their mutual national aims.

Beijing's Made in China 2025 policy, in particular, is driving technological specialisation within the high tech manufacturing sector as companies strive to move from global component suppliers to Chinese partnership manufactures. Supported with record research investment, the Made in China 2025 goals are obliging technical problem solving on a national scale.[125] Tsinghua University, one of China's top universities, announced plans in June 2017 to establish a laboratory to explore the integration of civil and military systems and cutting-edge technology innovation.[126]

The Australian defence, intelligence and security leaderships readily acknowledge the challenges, complexities, opportunities and threats that technological advances have brought to their areas of responsibility.

The Chief of the Defence Force, General Angus Campbell, said in February 2018:

> As with any approaching wave, there are choices in how we handle it. We can ignore it, pursuing 'more of the same' and risk being tossed around and left floundering in the wake. We can take a breath, dive under it and hope to come out on the other side, seeking time to assess which technologies we will acquire. Or we could start paddling now, riding the wave to secure an innovative and technological future.[127]

The Secretary of the Department of Home Affairs, Michael Pezzullo, said in June 2018:

> [W]e should perhaps see the associated race to attain national advantage in artificial intelligence and highly advanced computational capabilities as being as strategically significant as the race for naval mastery before the First World War, or the nuclear missile and space races during the Cold War …
>
> [W]e have to think anew about our workforce strategies, our use of technology, our posture on innovation, especially regarding artificial intelligence and machine learning, our business processes and practices, our risk models, and so on. It also follows that we need to think anew about the organisation of government—given the blurring of diplomacy, statecraft, intelligence, law enforcement, immigration, customs and border functions, and more besides, are our structures fit for purpose? We need to look again at how we align missions and functions and how we integrate effort across out-dated organisational boundaries.'[128]

Collectively, the defence, intelligence and security community administers a figure approaching $50 billion p.a. With the recent changes in the administrative structures covering the three domains, it's recognised that technological change is not only transforming society but reshaping how warfare, domestic security and intelligence gathering and analysis are conducted.

This level of funding, plus the sheer technological complexity of the issues being tackled, demands that the national security community has access to not only the best and the brightest minds available in Australia but takes a more robust approach to how it obtains its scientific and engineering counsel.

Currently, the security and intelligence agencies work through DSTG, which is located within the Department of Defence. The framework for this is set out in the National Security Science and Technology Policy and Priorities, which have been updated several times over the past decade.[129]

The organisational structure of the Home Affairs portfolio does not yet include an S&T or R&D directorate. Given its size and mandate, the Home Affairs Department needs such a structural function to direct and prioritise investment processes across the many R&D fields relevant to the broad portfolio. A similar arrangement should apply to the Office of National Intelligence.

Consideration should be given to systematising engagement practices with public and private S&T service providers across the national security community.[130]

As opposed to general industry policy in a free market economy, technological preparedness as it pertains to national security is primarily the responsibility of the federal government. Australia's innovation system has certain strengths and weaknesses, but, given the stated requirements of the national security R&D apparatus, it's clear that there are a few gears missing.

Missing gears

Turning scientific discoveries into practical applications is not our innovation system's strength. Australian industries and governments have simply not invested in direct technology transfer mechanisms. Fortunately, mechanisms Australia lacks that work for national security R&D exist in allied countries, and their adoption in Australia is feasible in terms of relative cost and continuity with national innovation progress to date.

Advanced research projects

As was identified as a strategic gap in our 2015 Special Report, Australia doesn't have Defence-led management and direction of basic and applied R&D projects within industry and academia. The reorganisation of past innovation programs under the Defence Innovation Hub and Next Generation Technology Fund programs is a positive incremental improvement on past collaborative innovation measures. In 2015, we estimated that 3% of the 2014 R&D budget was allocated to collaborative activities. Based on apparent activity rather than available budget details, collaborative investment appears to have increased, perhaps to 4% (in 2017). As we noted in 2015, several times that amount is needed to take real advantage of Australia's public and private innovative capacity. So, while additional resources have increased collaborative R&D activity, it appears that high-quality, high potential investment options remain unfunded.

Missing is a DARPA function (established in the US 60 years ago) to mine fundamental discoveries, accelerate their development and lower their risks until they prove their promise and can be adopted by the services. Our current arrangements largely kick in only when a technology has proved its purpose. In past decades, some of that capacity (budget, staff, risk appetite and industry outreach to advance projects from promising in-house research to valuable operational reality) existed within DSTO. The development and deployment of the Jindalee Operational Radar Network and the Nulka active missile decoy are conspicuous technological success stories that today's national security R&D system is now less able to replicate.

The scope of Australia's advanced research project support needs to be extended down to the fundamental discovery level, and across the Defence, Intelligence and Home Affairs portfolios.

Fast commercial and near commercial projects

> The DoD's relationship with Silicon Valley … will be one of these disgraceful chapters that will be written about. That's where the innovators are, sir.
>
> —US Senator John McCain, Chairman of the Senate Committee on Armed Services, November 2017, online.

The most innovative organisations in recent years have been tech-based start-up companies. This is because they're highly scalable, in that they offer IT-based products and services, which require little physical capital, to the world. It's also because the start-up sector has a high and fast failure rate. This creates a commercial ecosystem that affords frequent opportunities to a high number of potential ideas. Personnel within this ecosystem learn from their failures and move between tech companies and academia more frequently than average.

The traditional engagement method for defence contractors entails long lead, decision and step times. Hence, defence contractors are typically large to very large multinational corporations. Engaging start-ups and small companies will require a change in mindset to overcome base assumptions born from long experience with large contractors or false impressions of start-ups derived from the media.[131]

There's an opportunity to address this by establishing US DIU functions. Established in 2015 as 'DIU experimental', DIU provides non-dilutive capital in the form of pilot contracts for commercial innovation that solves US Department of Defense problems.[132] Importantly, engagement is fast and adds value to the company. Responses to DIU solicitations are provided within 30 days, and contracts are established in less than 90 days.[133] By providing non-dilutive capital, government regards success not as ownership or revenue, but as having the right new product developed and available.

Missing also is an MD5 function—the US armed services' National Security Technology Accelerator.[134] Established in 2016 as a public–private partnership, MD5 collaborates with US research entities to run education, collaboration and acceleration programs. Tools, training and access to Defense Department assets enable entrepreneurs outside and inside the defence organisation to develop and potentially commercialise innovative ideas.

While DIU develops technologies, MD5 develops research networks and communities of innovators to address national security problems. This education and community development function is critical to bridging the awareness gap between what government could need and what academia and industry could deliver. The mechanism also helps fast-track the development of trust between would-be providers and national security users. Driven by the services, MD5 also works with, and welcomes, unsolicited proposals.

Lessons from national security focused participants in general start-up accelerator programs should inform the design of a dedicated national security start-up support mechanism. For example, CSIRO's ON accelerator has various programs to develop Australian research into ventures and has run an accelerator experience for defence-related innovators.[135]

The US In-Q-Tel venture capital firm serves as a proven model for investment in national security focused 'development' that serves the intelligence community.[136] As a not-for-profit venture capital firm with appropriate clearance and security arrangements, In-Q-Tel seeks out and supports emerging IT-based ideas and tools. Founded in 1998, In-Q-Tel invests in start-ups working on genetics, commercial space, communications, cyber tech, data analytics, infrastructure, the internet of things, materials, electronics, power and energy.

The scope of Australia's national security start-up engagement needs to be systematised to match the opportunity-oriented, fail-fast nature of start-ups and function across the defence, intelligence and home affairs portfolios. Missing is a government-supported venture capital mechanism to help grow start-ups that have or could have national security application.

Whole-of-government coordination

> Our response will be to prioritize speed of delivery, continuous adaptation, and frequent modular upgrades. We must not accept cumbersome approval chains, wasteful applications of resources in uncompetitive space, or overly risk-averse thinking that impedes change. Delivering performance means we will shed outdated management practices and structures …
>
> —Summary of the 2018 *National Defense Strategy of the USA: sharpening the American military's competitive edge*, January 2018, online.

Legacy departmental arrangements are a dated framework for national security R&D. The creation of the Department of Home Affairs brings many elements together, which has benefits, but the necessity to establish an efficient national security R&D system demands a whole-of-government approach.

The strategic coordination and advisory space can be addressed by establishing a National Security S&T Advisory Committee made up of eminent scientists, engineers, technologists and entrepreneurs. The US and the UK have boards and committees drawn from or based in their national academies, as well as successful innovators from industry. The US Defense Science Board produces annual reports and topical reports (classified and unclassified), which enables strategic planning across the public and private US national security R&D sectors.

Missing at the coalface are S&T directorates or similar in the Department of Home Affairs and Office of National Intelligence, to work with DSTG in the Department of Defence or with other government agencies, such as CSIRO. A cross-portfolio network would also provide stability to national security R&D leadership, as reliance upon senior personnel in one portfolio is prone to discontinuities.[137]

A strategic plan for national security R&D personnel is needed to ensure the ready availability of high-quality talent for governments, research entities and the private sector.

Priority for national security R&D

Across the wide range of Australia's research, innovation, taxation, departmental and industry policies, R&D pursuant to national security interests is not a distinct priority. Past national research priorities have included national security, but no longer. National security R&D needs to be added to the various goals, drivers and objectives across industry, research entities and government. More important than what its ranking should be is that it must exist as a priority.

Following on from a strategic priority for national security R&D should be the means to enable its delivery. Forecast real and relative declines in defence R&D budgets and underpowered whole-of-government organisation suggest that resourcing is missing from the system. As established above, global R&D trends suggest that it's imprudent to maintain policy settings and investment levels that lead to a real and relative decline of our technological advantage, self-reliance and preparedness.

Productive R&D requires a critical mass of activity. Multinational business R&D is heavily concentrated in the largest firms. Investment typically takes the form of collaborative arrangements (including subcontracting) with national research entities, a long-term financial commitment of over US$40 million p.a. and aggressive staff recruitment and retention policies. Big business asks, 'Will this R&D investment make a big difference?' Governments should do the same.

Authoritarian countries are able to direct both their industry and their government research entities to advance strategic (military and security) R&D subjects. Importantly, only a small proportion of overall national R&D efforts need be directed at particular challenges in order to achieve a critical mass of R&D focus, such as that which is now blunting Western defence and security technological strengths.

Options

Just as our national innovation system is as much evolved as planned, so too are arrangements for national security R&D. Fortunately, for the size of the gaps in our national security R&D framework, there exist proven models that can address the identified shortcomings.

An Australian ARPA

An Australian Advanced Research Projects Agency (Australian ARPA) should be established as a statutory authority to meet the needs of defence, intelligence and home affairs. Reporting to the three relevant ministers and their departmental secretaries, the Australian ARPA would operate according to the US DARPA model. A nominal budget, proportional to Australia's defence, intelligence and home affairs expenditure, S&T needs and broader national R&D base,[138] would be around $300 million p.a. Next Generation Technology Fund programs and expertise would be subsumed into the Australian ARPA and carry on. DARPA expertise should be called upon to establish the agency with seconded staff.

National security innovation hubs

The Defence Innovation Hub has met with early success but should be expanded to include functions akin to those deployed by DUI and MD5, the US armed services' National Security Technology Accelerator. Accordingly, the nominal budget should be increased to at least $100 million p.a.

The 2017 IIR soundly recommended the establishment of an Intelligence Community Innovation Hub. The hub should enable novel, collaborative activities, such as In-Q-tel functions.

Critically, the Department of Home Affairs should establish a Home Affairs Innovation Hub with functions similar to those recommended for the Defence Innovation Hub. Accordingly, the nominal budget should be increased to at least $50 million p.a.

National security innovation hubs should invest in systems (such as AI systems) to stay abreast of international S&T trends and developments.

Whole-of-government coordination

Given the size of Australia's national security investment and to ensure systematic and thorough coverage, the existing departments' and agencies' S&T Advisory Committee arrangements should be combined. A National Security S&T Advisory Committee would jointly provide advice and service for the Defence, Intelligence and Home Affairs portfolios. Composed of eminent scientists, engineers, technologists and entrepreneurs who cover the full span of fields relevant to the portfolios, the committee would serve the three communities and government on matters of science, technology, research and development. With the support of a dedicated secretariat, the committee could also operate portfolio subcommittees to provide portfolio-specific advisory services.

While the three communities have different but overlapping needs, the matters of science, technology, research and development are common, as are the avenues through which they may be developed. Whole-of-government coordination and cooperation will ensure that limited resources are appropriately (strategically) applied without overlap.[139]

The government should establish S&T directorates for the Department of Home Affairs and the Office of National Intelligence with a remit to manage S&T policy and activities within their portfolio responsibilities. By establishing new directorates, the respective communities would be afforded dedicated foresighting and strategic planning functions that will be needed to ensure that the portfolios retain their leading technological edge in coming years.

With sector-wide consultation, the government should develop a strategic plan for national security R&D personnel. The plan should start with a discussion paper to familiarise stakeholders with the challenges and potential solutions. Sector engagement through written feedback and roundtable consultations should culminate in a strategic plan of action for sector organisations. That process would take 18 months. The plan would cover career path resilience; training and modernisation; security clearance portability; gender and diversity issues; future proofing and demographic profiles; qualifications and skills projections; and allied and government research entity – industry exchanges.

Reset national security R&D priorities

The various national R&D priorities need to be reset to take in national security R&D. National security isn't currently listed as a priority area for research funding by the ARC and the NHMRC. While funding demarcation might not be necessary, it would be productive if national security objectives, outcomes and aims were at least mentioned so as to give the research community a funding framework within which national security aspects may add to the prospects of grant success.

Basic research relevant to Australia's national security shouldn't displace current work. Constantly shifting research priorities have hampered Australian R&D over the past 20 years. Additional funding (~$200 million p.a.) is needed to provide critical-mass support for strategically relevant basic research. The erosion of Australia's defence and security technological advantage will continue unless new investment is made in obvious fields, such as AI.

Investment in strategically significant areas is needed to make a significant difference, but the scale of that investment, both in time and in expenditure, needs to be of a critical mass. Special translation funds such as the government's Biomedical Translation Fund (a $500 million venture capital scheme funded by government and private-sector superannuation funds) was rightly judged to be at a scale to be effective. Such risk capital and translational S&T expertise is needed to capitalise on the results of government investment in research over the past several decades.

Given the importance that the government has attached to positioning Australia as one of the world's top 10 global defence exporters within the next decade,[140] the government may wish to extend the same sort of R&D tax treatment to the defence industry sector as it has done for Australia's medical research community. Similarly, the ability to write off R&D investment (given the small market and high failure rates of projects, tenders and start-ups) would help build the sector's capacity—R&D and innovative ideas need to fail at a certain rate in order to develop the system's capacity to deliver productive R&D.

Reconsideration of the government's decision to tighten the criteria for eligible R&D tax concessions is also warranted. One remedy would be the application of a medical research company type annual refund cap for companies and research entities working in areas pertinent to the three communities' interests. As defence, intelligence and security are three of Australia's highest priorities, there may be commensurate signals to encourage firms to undertake R&D in those fields.

AI is one S&T field that stands out as requiring special attention. Australia's national security advantage is arguably being eroded most quickly by this technology. As AI is an enabling technology with potential to affect aspects of national security, consideration of significantly greater investment in AI R&D and implementation is required.

Finally, to enable national security R&D sector-wide coordination, consideration should be given to the annual publication of an R&D guidance document, including a capability forecast, that industry and academia could use to develop capacities to bring forward new research ideas and solution sets. This should include the publication of an annual account, emulating the UK approach but perhaps extended to include a disclosed S&T component to further assist industry and academia in bringing forward solution sets germane to the various agencies' interests.

CONCLUSIONS

Global pre-eminence, which began with gunboat diplomacy in the early 19th century, is enabled by technology. Current technological trends suggest that the ownership of clearly dominant technology by Europe and its former colonies will end sometime in the second quarter of the 21st century. As a top 10 country in research capacity, Australia has an exceptional sovereign asset that stands to be leveraged to sustain our national security strength. We need to find the ambition.

Over the past decade, Australian innovation has stagnated, and we've been overtaken by better performing nations. Government defence R&D as a percentage of the Defence budget continues to decline, and is now budgeted to be less than 1% (0.98%) by 2020–21. In 2015–16, the business share of defence R&D had fallen to 28.8%, down from a high of 45.1% in 2004–05. It's too soon to say whether recent and welcome defence industry and innovation policies have altered those trends.

Despite the diminishment of Australia's S&T advantages by globalisation, current policy involves a reduced investment in R&D, including national security R&D. Recent policy (the National Innovation and Science Agenda) is beginning to address longstanding low levels of private-sector investment, industry–academia collaboration and local venture capital. A similar policy refresh is needed for national security R&D. It would certainly support the ambitions of 2016 Defence Industry Policy and the recommendations of the 2017 IIR.

The mid-2018 ASPI – Ai Group National Security R&D Survey found that industry and academia were strong in their praise for the government's 2016 Defence Industry Policy Statement, and a large majority of respondents reported that the implementation of the initiatives are having a medium to high level of impact. Criticisms were voiced about engagement and response time (considered too slow), lack of medium- to long-term detail on which to plan and minimal attention to R&D outside the Defence portfolio. The 2018 Budget announced a tightening of the R&D tax incentive, which raised serious concerns about ongoing government commitment, which hinders R&D planning. Start-ups noted that R&D tax arrangements were problematic, given their cash-flow model, and noted that bespoke exemptions offered for clinical medical trials should also be offered for national security reasons.

Since the 2015 Special Report, other analysts have suggested that Australia has use for a DARPA[141] functionality and, since the US DIU's successful establishment,[142] for a similar functionality to engage with start-ups. We agree, and also conclude that MD5 functionality is warranted to overcome the sizeable gap between what government departments and agencies could need and what academia and industry could deliver. Bridging that gap requires education and community development on all sides, as well as resources and policy certainty. As a precursor to typical tech accelerator operations, MD5 has programs that educate and develop the R&D ecosystem to serve the innovation needs of the US armed services.

A national strategy for the national security R&D workforce is needed. The centre of Australia's R&D strength is the quality and skills of its problem solvers. Attractive career frameworks for Australian talent are a prerequisite for efficient R&D, which means taking concrete steps to break down mobility barriers between governments, industry and research entities.

The *Australia 2030: prosperity through innovation* report recommended that Australia 'increase the use of mission-directed support'. However, Australia has lost sight of the national security R&D mission. Because mission-oriented R&D produces results and because national security is a primary responsibility of the federal government, a mission approach should be taken. We suggest the following options to carry out such a mission:

- The establishment of an Australian ARPA to service the Defence, Intelligence and Home Affairs portfolios would facilitate transformative innovation. Agile R&D ecosystem building would be achieved by bolstering the Defence Innovation Hub with US DIU-like functions and MD5-like functions. Replicating the innovation hub model for Home Affairs and establishing an innovation hub for intelligence would provide similar benefits for those sectors.
- Whole-of-government coordination could be improved by combining existing national security departments' and agencies' S&T advisory arrangements, and augmenting them as necessary, to form a National Security S&T Advisory Committee to jointly service the Defence, Intelligence and Home Affairs portfolios. To drive R&D and general innovation, S&T directorates should be established in the Office of National Intelligence and in Home Affairs.
- A strategic plan for national security R&D human resources should be developed collaboratively between government, industry and research entities and cover personnel training pipelines; career paths; security clearances; intrasector mobility; gender and diversity; qualifications; and allied and sectoral exchanges.
- The government should review priorities across all government R&D delivery and grant agencies to include national security. National security, as appropriate according to whole-of-government objectives, needs to appear at some level in all government research investment priorities. Similarly, special consideration in taxation treatment should be afforded, at some level, to national security related R&D in industry.
- Further investment in strategically relevant fields (AI is the most obvious example) is needed to make a difference significant enough to arrest the erosion of Australia's defence and security technological advantages. Consideration is needed to determine what constitutes the critical-mass investment to at least sustain Australia's technological advantage over the long term. This includes investment in R&D infrastructure. To enable national security R&D sector-wide coordination, consideration should be given to the annual publication of a national security R&D guidance document, including capability forecasts, that industry and academia can use to develop capacities to bring forward new research ideas and solution sets.

Alternatives to these options surely exist but, just as surely, business-as-usual will guarantee the continued erosion of Australia's defence and security technological advantage. If that happens, we'll eventually be obliged as a nation to choose between our economic and security standing, as securing both will no longer be practical. Significant policy revision and strategic investment are needed to take advantage of the opportunities afforded by being a world-leading research nation. The policy option to leverage this sovereign advantage is evaporating and may be gone within a decade.

NOTES

1 Paul Dibb, 'New security reality demands new Australian Policy', *The Strategist*, 23 July 2018, online.
2 Australian Bureau of Statistics (ABS) and Defence Portfolio Budget Statements.
3 Malcolm Turnbull, 'A strong and secure Australia', media release, 18 July 2017, online.
4 Organisation for Economic Co-operation and Development (OECD), 'Main science and technology indicators', *OECD.Stat*, online.
5 National Science Foundation, *2018 digest: global R&D: one measure of commitment to innovation*, online.
6 Bill Gates, Melinda Gates, 'The 10 toughest questions we get', *GatesNotes*, 2018, online.
7 Homi Kharas, 'The unprecedented expansion of the global middle class: an update', *Brookings*, online.
8 Sensis, *Sensis social media report, 2017*, 'Chapter 1: Australians and social media', 22 June 2017, online.
9 David Cowling, 'Social media statistics Australia—January 2018', *SocialMediaNews.com.au*, 1 February 2018, online.
10 *Australian video viewing report, Quarter 4 2017*, Regional TAM, OzTAM, Nielsen, 2018, online.
11 'Percentage of global research and development spending in 2018, by industry', *Statista*, 2019, online (paywall).
12 '2017 global R&D funding forecast', *R&D Magazine*, Winter 2017, online.
13 The Apollo program (1959–1973), which developed much of its own technology, cost $156 billion in 2018 dollars.
14 Melanie Oppenheimer, Debbie Haski-Leventhal, Kirsten Holmes, Leonie Lockstone-Binney, Lucas Maijs, 'Where have all the volunteers gone?', *The Conversation*, 24 September 2015, online.
15 '8 out of 10 Australians say loneliness is increasing: new survey', media release, Lifeline, 2016, online; Calla Wahlquist, 'Eighty-two per cent of Australians say loneliness is increasing, Lifeline survey finds', *The Guardian*, 27 September 2016, online.
16 The results of the US Special Counsel investigation into Russian interference in the 2016 US elections will illuminate the extent of these types of incursion, as deployed in 2016. The results of the investigation will need to be considered in the light of near-future technological capabilities and scale change between the capacities of a small data technology company (such as Cambridge Analytica) and the combined resources of a nation-state.
17 '2017 Edelman Trust Barometer', *Edelman*, 21 January 2017, online.
18 Lowy Institute, *Lowy Institute poll 2018: democracy*, online.
19 World Bank, *China: systematic country diagnostic*, report no. 113092-CN, 2017, online.
20 UNESCO, 'A decade of investment in research and development (R&D): 1990–2000', *UIS Bulletin on Science and Technology Statistics*, April 2004, online.
21 ABS, *Research and experimental development, all sector summary, Australia, 2004–05*, cat. no. 8112.0, ABS, Canberra, online.
22 OECD, 'Main science and technology indicators', 2017(1), *OECDiLibrary*, online.
23 ABS, *Research and experimental development, businesses, Australia, 2015–16*, cat no. 8104.0, ABS, Canberra, online.
24 'Academic ranking of world universities', 2005, *Shanghai Ranking*, online.
25 'Academic ranking of world universities', 2017, *Shanghai Ranking*, online.
26 '2017 global R&D funding forecast', *R&D Magazine*, Winter 2017, online.
27 ABS, *Research and experimental development, businesses, Australia, 2015–16*.
28 Michelle Jamrisko, Wei Lu, 'The US drops out of the top 10 in innovation ranking', *Bloomberg*, 23 January 2018, online.
29 OECD, 'OECD science, technology and industry scoreboard 2017', *OECDiLibrary*, online.
30 Shaped by history and natural heritage, our colonial university system has grown pursuant to traditional academic excellence and demand for tertiary education, in particular from fee-paying students from nations in economic transition. Our resources and agriculture sectors have prospered with relatively modest R&D investment, while the services sector (now contributing 70% of GDP and employing 80% of Australians) has grown rapidly, enabled by our high level of technological literacy.
31 Steve Millward, 'China sees record tech funding in 2017', *TechInAsia*, 5 January 2018, online.
32 A unicorn company is a privately held start-up valued at over US$1 billion. Australia has one: Canva. Xie Yu, Maggie Zhang, 'At the heart of China's techno-nationalism is a hit list of 200 unicorns', *South China Morning Post*, 31 March 20128, online.
33 OECD, 'Main science and technology indicators', *OECD.Stat*, online.
34 OECD, *A decade of investment in research and development (R&D): 1990–2000*, online.

35 Leading R&D teams are multinational and multidisciplinary, and are typically led by and strategically staffed with people educated, trained and professionally experienced in Europe, North America, Japan, South Korea, Australia and New Zealand.
36 UNESCO, *How much does your country invest in R&D?*, UNESCO Institute for Statistics, online.
37 James R Clapper, 2016, 'Statement for the record: Worldwide threat assessment of the US intelligence community', Senate Armed Services Committee, 9 February 2016, 1, online.
38 Paul Dibb, Richard Brabin-Smith, *Australia's management of strategic risk in the new era*, ASPI, Canberra, online.
39 From 1.5% of $2.2 trillion globally in 2018 to about 0.8% of $5 trillion globally in 2030.
40 ABS, *Research and experimental development, businesses, Australia, 2015–16*.
41 ABS, *Research and experimental development, government and private non-profit organisations, Australia, 2016–17*, cat. no. 8109.0, ABS, Canberra, 5 July 2018, online.
42 Defence Science and Technology Organisation, *DSTO annual review, 2013–14*, Australian Government, Canberra, 2014, online.
43 2018 Senate Estimates Question On Notice 113: — 88% of staff in S&T roles; 12% in business and administration roles; 77% men and 23% women, with an average age 47 years.
44 ABS, *Research and experimental development, businesses, Australia, 2015–16*; Deloitte Access Economics, *ACS: Australia's digital pulse: driving Australia's international IT competitiveness and digital growth*, 2018, online.
45 ABS, *Research and experimental development, higher education organisations, Australia, 2016*, cat. no. 8110.0, ABS, Canberra, 22 May 2018, online.
46 Australian Government, *2017 Independent Intelligence Review*, June 2017, online.
47 Department of Home Affairs, *Blueprint for Home Affairs*, Australian Government, Canberra, 2018, online.
48 Department of Immigration and Border Protection, *Annual report, 2014–15*, 'Secretary's review', Australian Government, Canberra, 2015, online.
49 Excluding ASIO's unpublished R&D investment.
50 Department of Homeland Security, *Science and Technology Directorate: budget overview, fiscal year 2019 congressional justification*, US Government, online.
51 Born from DSTO, the centre moved to the Department of the Prime Minister and Cabinet in 2012 to assume whole-of-government responsibilities. In 2015, the centre moved back to Defence. It currently has staff of about 12.
52 Defence Science and Technology Group, *National security science and technology: policy and priorities*, Australian Government, Canberra, 2018, online.
53 It's desirable that this inaugural survey becomes a periodical series. Response rates would improve to a point of confident representation, which would provide the sector and policymakers with an accurate understanding of conditions and prevailing trends.
54 DIIS, *Australian innovation system report 2017*, Australian Government, Canberra, November 2017, online.
55 The Treasury, *Research & development tax incentive amendments: key documents*, 2018, online.
56 'Submissions', *StartupAUS*, online.
57 Jill Aitoro, 'The next Sputnik: here's why US stands to lose technological edge to China', *DefenseNews*, 2 December 2017, online.
58 Since 2000, China's spending on R&D has grown by an average of 18% each year, while that of the US has grown by only 4%. Maria T Zuber, 'Falling short on science', *New York Times*, 26 January 2018, online.
59 Vasilis Trigkas, 'China has its DARPA, but does it have the right people?', *The Diplomat*, 9 August 2017, online.
60 Sebastian Sprenger, 'Germany wants its own version of DARPA, and within a year', *DefenseNews*, 18 July 2018, online.
61 Jeffrey M Perkel, 'The hackers teaching old DNA sequencers new tricks', *Nature*, 24 July 2018, online.
62 Mark Ware, Michael Mabe, *The STM report: an overview of scientific and scholarly journal publishing*, 4th edition, March 2015, online.
63 Arif E Jinha, 'Article 50 million: an estimate of the number of scholarly articles in existence', *Learned Publishing*, July 2010, 23(3):258–263, online.
64 Mathieu Rosemain, Michel Rose, 'France to spend $1.8 billion on AI to compete with China, US', *Reuters*, 30 March 2018, online.
65 *AI for Humanity*, online.
66 'France prepares 1.5 billion euro push to foster AI research', *Phys.org*, 29 March 2018, online.
67 '"Whoever leads in AI will rule the world": Putin to Russian children on Knowledge Day', *RT*, 1 September 2017, online; Tom Simonite, 'For superpowers, artificial intelligence fuels new global arms race', *Wired*, 9 August 2017, online.
68 Samuel Bendett, 'In AI, Russia is hustling to catch up', *Defense One*, 4 April 2018, online.
69 Sydney J Freedberg, 'Google helps Chinese military, why not US? Bob work', *Breaking Defense*, 26 June 2018, online; Charlotte Gao, 'Google stumbles back to China', *The Diplomat*, 16 January 2018, online.
70 Paul Mozur, 'Beijing wants AI to be made in China by 2030', *New York Times*, 20 July 2017, online; Zuber, 'Falling short on science'.
71 Mozur, 'Beijing wants AI to be made in China by 2030'.
72 David Cyranoski, 'China enters the battle for AI talent', *Nature*, 17 January 2018, online.
73 The University of Technology, Sydney ranked 30th, the Australian National University ranked 76th, the University of NSW ranked 81st, and National ICT Australia Ltd ranked 93rd.
74 'China's AI ambitions revealed by most cited research papers', *Financial Times*, 2 November 2017, online (paywall).
75 Greg Allen, Taniel Chan, *Artificial intelligence and national security*, Belfer Centre, July 2017, online.
76 Kelsey D Atherton, 'For the Defense Innovation Board, the future of AI is more than JAIC', *C4ISRNET*, 12 July 2018, online.

77 Lieutenant General Rick Burr, statement on 'Accelerated warfare', 8 August 2018, online.
78 Fiona Beardmore, 'Australian H&MR research facts', *Research Australia*, 21 January, 2016, online.
79 Timothy Dyke, Warwick P Anderson, 'A history of health and medical research in Australia', *Medical Journal of Australia*, 2014, 201(1 Suppl):S33–S36, online; National Health and Medical Research Council (NHMRC), *Funding*, no date, online.
80 'Research matters 2018, *Research Australia*, 9 January 2019, online.
81 Centers for Disease Control and Prevention, *Influenza (flu)*, 24 May 2018, online.
82 Emily Baumgaertner, '"We're out of options": doctors battle drug-resistant typhoid outbreak', *New York Times*, 13 April 2018, online; Nicola Davis, 'Antibiotic resistance crisis worsening because of collapse in supply', *The Guardian*, 31 May 2018, online.
83 World Health Organization, *World Antibiotic Awareness Week, 14–20 November 2016: 2016 campaign kit*, online.
84 Nicholas Wade, 'Scientists seek moratorium on edits to human genome that could be inherited', *New York Times*, 3 December 2015, online.
85 Julie Anne Schuck, *Social and behavioral sciences for national security*, 'Preface', National Academies Press, 2017, online.
86 Cochlear, *History*, 2019, online.
87 Larry Hardesty, 'Computer system transcribes words users "speak silently"', *MIT News*, 4 April 2018, online.
88 'Brain computer interface market—industry trends, opportunities and forecasts to 2023', *Researchandmarkets.com*, December 2017, online.
89 Emotiv, *Emotiv: about us*, no date, online.
90 'TOP500 list, June 2018', *Top 500: the list*, online.
91 Steve Lohr, 'China extends lead as most prolific supercomputer maker', *New York Times*, 25 June 2018, online.
92 Australian Government, *Facilities for the future: underpinning Australia's research and innovation*, no date, online.
93 Biosecurity measures received an additional allocation of $0.4 million over forward estimates.
94 DIIS, *Growth centres*, Australian Government, Canberra, 12 December 2018, online.
95 ARC, *Science and Research Priorities*, Australian Government, Canberra, 12 June 2018, online
96 NHMRC, *NHMRC Corporate Plan 2017–2018,* Australian Government, Canberra, August 2017, online.
97 'Strong start for VC market in 2018: US$49.3bn invested worldwide', media release, KPMG, 12 April 2018, online.
98 Australian Government, *Defence industry and innovation programs update report 2017*, Australian Government, Canberra, 7 May 2018, 6, online. A portfolio of legacy innovation projects worth approximately $61.2 million was transitioned into the Defence Innovation Hub, such as the long-running and successful Capability Technology Development Scheme.
99 Department of Defence ministers, *All media releases*, Australian Government, online. Information on program expenditure is not publicly available. Estimates are taken from funding announcement media releases. The *Defence industry and innovation programs update report 2017* (released May in 2018) provides some data but is narrative.
100 Christopher Pyne, 'Defence partners with industry to develop innovative capability for Army, media release, 21 June 2018, Australian Government, Canberra, online.
101 Australian Government, *Defence industry and innovation programs update report 2017.*
102 Christopher Pyne, 'Australian and US universities to collaborate on defence research', media release, 24 May 2016, Australian Government, Canberra, online.
103 Department of Defence, '$25 million for Australian universities to work with top US counterparts', media release, Australian Government, Canberra, 23 May 2017, online.
104 Mark Dodgson, David Gann, *The missing ingredient in innovation: patience*, World Economic Forum, 26 April 2018, online.
105 HM Treasury, *Financing growth in innovative firms: consultation response*, UK Government, November 2017, online.
106 Patient Capital Review Industry Panel, *Patient Capital Review: industry panel response*, UK Government, October 2017, online.
107 British Business Bank, *National Security Strategic Investment Fund (NSSIF) Programme: guidance document*, July 2018, online.
108 UK Government, *National Security Capability Review*, March 2018, online.
109 Matt Hourihan, David Parkes, *Guide to the President's Budget: Research & Development FY 2019; A review and summary of R&D funding proposals in the White House budget request for the 2019 fiscal year.*, American Association for the Advancement of Science, 31 May 2018, online.
110 John Louth, Chrisian Moelling, *Technological innovation: the US third offset strategy and the future transatlantic defense*, policy paper, Armament Industry European Research Group, December 2016, online.
111 Lauren C Williams, 'DIUx gets a big boost in FY19 budget', *FCW*, 12 February 2018, online.
112 Brendan Thomas-Noone, *Mapping the third offset: Australia, the United States and future war in the Indo-Pacific*, US Studies Centre at the University of Sydney, 5 December 2017, online.
113 'FY 2019 R&D appropriations dashboard', American Association for the Advancement of Science, no date, online.
114 Michael Hoffman, 'Mattis plans to bolster DIUX', *Defense Systems*, 31 August 2017, online.
115 'Remarks by Secretary Mattis on the launch of the US National Defense Strategy', US Department of Defense, January 2018, online.
116 Department of Defence, *External security vetting services*, discussion paper, 2018, online.
117 'Hedge funds fight back against tech in the war for talent', *Financial Times*, 2 August 2018, online (paywall).
118 *Crossroads 2017*, StartupAUS, 2017, https://startupaus.org/document/crossroads-2017/.

119 Defence Science and Technology Organisation, *DSTO annual review 2013–14*, Australian Government, Canberra, online; 2018 Senate Estimates Question On Notice 113: —88% of staff in S&T roles; 12% in business and administration roles; 77% men and 23% women, with an average age 47 years.

120 Naval Group, *Financial report 2017*, online.

121 Naval Group, 'Flinders University and 4 French schools of engineering enter defence partnership', media release, 17 January 2017, online; Flinders University, 'French scholarships highlight Flinders leadership', news release, 3 July 2018, online.

122 US Government, *National Security Strategy of the United States of America*, December 2017, online.

123 Lowy Institute, Asia Power Index, online.

124 DIIS, *Australia 2030: prosperity through innovation*, Australian Government, November 2017, online.

125 Chinese Minister of Science and Technology Wan Gang announced in February 2018 that China spent US$279 billion on R&D in 2017 (industry 77% and government 23%, or US$64 billion). 'China spends $279 bln on R&D in 2017: science minister', *Reuters*, 27 February 2018, online.

126 'Tsinghua launches the establishment of a military–civilian integrated cutting-edge defence technology laboratory', *Tsinghua University News*, 26 June 2017, online.

127 Lieutenant-General Angus Campbell, address to the *Australian Defence Magazine* Congress, 14 February 2018, online.

128 Michael Pezzullo, address to the International Summit on Borders, Washington DC, 19 June 2018, online.

129 Defence Science and Technology Group, *National security science and technology: policy and priorities*.

130 In the UK, departmental scientific advisers help coordinate engagement with universities and industry in relation to S&T procurement.

131 Jeff Decker, 'Renewing defense innovation: five incentives for forming Pentagon–startup partnerships', *War on the Rocks*, 3 May 2018, online.

132 Non-dilutive capital, sometimes known as 'non-dilutive financing' or 'non-intrusive capital', is capital received by start-ups to grow or specialise without affecting (diluting) equity ownership. The benefit for a non-dilutive investor is not ownership but the creation of a unique and needed product or service. Priority commercial access is typically agreed.

133 Defense Innovation Unit, Work With Us (webpage), US Department of Defense, US Government, accessed December 2018, online.

134 MD5 beta, *About MD5*, no date, online.

135 CSIRO, *How ON works*, no date, online.

136 IQT: in Q tel, *Insights & access*, no date, online.

137 Since 2015, the Defence portfolio has had one Chief Defence Scientist (Zelinski, March 2012 - November 2018), three Defence ministers (Andrews, Payne and Pyne) and one (assistant) Minister for Defence Materiel and Science (Brough). Defence Minister Payne had carriage of defence S&T for almost 3 years. This was the longest period of stable Minister - Chief Defence Scientist leadership since 2000 (the average duration between 2000 and 2015 was 11 months).

138 Compared to US (DARPA, HSARPA, IARPA) and UK S&T R&D arrangements.

139 A criticism of US Government R&D programs.

140 Christopher Pyne, 'Launch of job-creating Defence Export Strategy', media release, 29 January 2018, online.

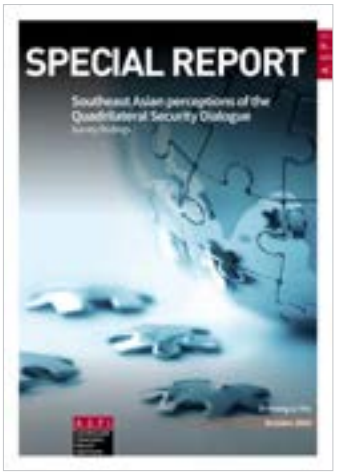
141 Michael J Biercuk, *Next steps for Australia's defence innovation: lessons from DARPA*, US Studies Centre at the University of Sydney, 12 October 2017, online; Peter Jennings, 'With Trump at large, Australia needs a Plan B for defence', *The Australian*, 21 July 2018, online.

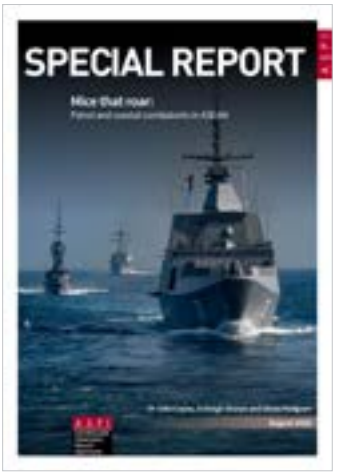
142 Daniel Kliman, *Now is the time to take DIUX global*, US Studies Centre at the University of Sydney, 24 May 2018, online.

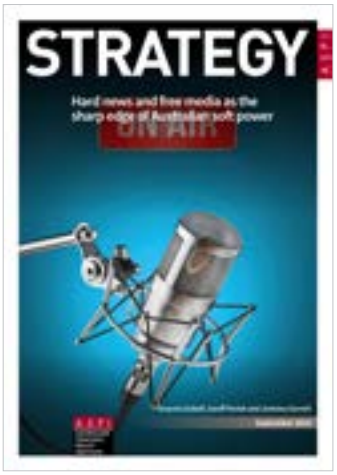
ACRONYMS AND ABBREVIATIONS

ABS	Australian Bureau of Statistics
ADF	Australian Defence Force
AI	artificial intelligence
Ai Group	Australian Industry Group
ARC	Australian Research Council
CSIRO	Commonwealth Scientific and Industrial Research Organisation
DARPA	Defense Advanced Research Projects Agency (US)
DIU	Defense Innovation Unit (US)
DSTG	Defence Science and Technology Group
DSTO	Defence Science and Technology Organisation
EU	European Union
GDP	gross domestic product
GERD	gross expenditure on R&D
GII	Global Innovation Index
ICT	information and communications technology
IIR	Independent Intelligence Review
IT	information technology
MIT	Massachusetts Institute of Technology
national security R&D	defence, security and intelligence services R&D
NHMRC	National Health and Medical Research Council
OECD	Organisation for Economic Co-operation and Development
ONI	Office of National Intelligence
PPP	purchasing power parity
R&D	research and development
S&T	science and technology
UK	United Kingdom

Some recent ASPI publications



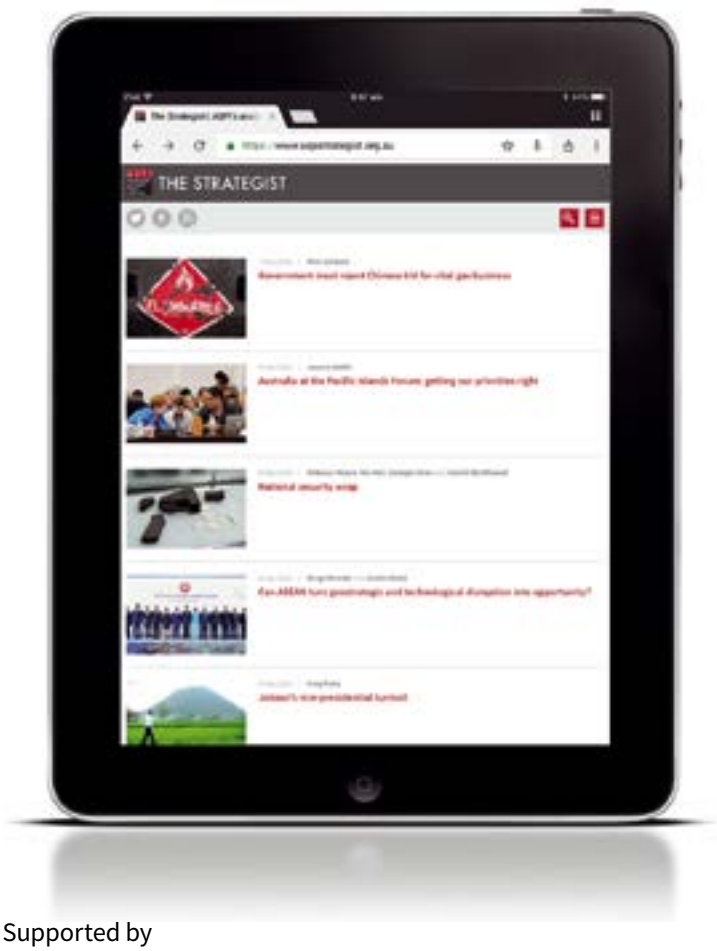




WHAT'S YOUR STRATEGY?

Stay informed via the field's leading think tank, the Australian Strategic Policy Institute.

The Strategist, ASPI's commentary and analysis website, delivers fresh ideas on Australia's defence and strategic policy choices as well as encouraging discussion and debate among interested stakeholders in the online strategy community. Visit and subscribe to an email digest at www.aspistrategist.org.au.



facebook.com/ASPI.org

@ASPI_org

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

Supported by

LOCKHEED MARTIN THALES

To find out more about ASPI go to www.aspi.org.au or contact us on 02 6270 5100 and enquiries@aspi.org.au.

Defence and security R&D:
A sovereign strategic advantage

ISSN 2200-6648