# 4. Australia

Australia's cyber-security strategies have concentrated on national security, commercial cyber security, the industrial base for sovereign capability, workforce development and good international citizenship. The Australian Signals Directorate, the country's principal cyber-related agency, remains the most influential in national policymaking. The country is still developing its military cyber strategies and policies after setting up an Information Warfare Division in 2017. Australia can boast some research and industry credentials in the field of information and communications technology and cyber security, but these are growing from a low base. In part because of its 70-year membership of the Five Eyes intelligence alliance, Australia has more mature cyber capabilities than its modest defence and intelligence budgets might suggest. It is active in global diplomacy for cyber norms and cyber capacity-building. In 2016 it acknowledged for the first time that it possessed offensive cyber capabilities – examples of their use against the Islamic State (also known as ISIS or ISIL) were subsequently put into the public domain. Australia has actively supported the United States-led Cyber Deterrence Initiative, which aims to use cyber means to counter the malign cyber activity of other states. For Australia to become a more effective cyber power, it will need to make dramatically greater investments in cyber-related tertiary education and carve out a more viable sovereign cyber capability.

## Strategy and doctrine

Australia's first Cyber Security Strategy, released in 2009,[1] was the result of a review of 'e-security' the previous year. It had two main initiatives: to create an official national Computer Emergency Response Team to complement or supersede the one that had been operating since 1994, which was based in a university;[2] and to establish a national Cyber Security Operations Centre. But the document consisted largely of rhetorical policies – laudable intentions around topics such as shared governmental and private-sector responsibility, facing the increasing threats, protecting Australian values, identity protection, expanding and upskilling the cyber workforce, and enhancing international collaboration. It did not propose significant new investments in support of its rhetorical commitments, except in the area of national security.

In April 2016 the government launched a new Cyber Security Strategy.[3] Subtitled 'Enabling Innovation, Growth and Prosperity', the plan was as much about better exploiting the economic opportunities of the information age as it was about security. The security-related themes were familiar from the existing strategy

**List of acronyms**

| | |
|---|---|
| **ACSC** | Australian Cyber Security Centre |
| **ADF** | Australian Defence Force |
| **ASD** | Australian Signals Directorate |
| **ASIO** | Australian Security Intelligence Organisation |
| **DSCC** | Defence Signals Intelligence and Cyber Command |
| **ICT** | information and communications technology |
| **IWD** | Information Warfare Division |

documents of other countries, such as the United States, the United Kingdom and France: detect, deter and respond to threats in cyberspace, including through better anticipation of risks.[4] However, in comparison with previous strategies, the tone was more urgent. The document included a large number of new approaches to security, particularly around information-sharing between government and the private sector. It also acknowledged for the first time the government's use of offensive cyber capabilities to deter or respond to malicious cyber attacks.

Within 18 months, however, the planning processes for cyber strategy in the civilian sector were thrown into temporary disarray by major structural reforms that included changes to the status of the Australian Signals Directorate, the Australian Security Intelligence Organisation, the Australian Cyber Security Centre and the Attorney General's Department in order to carry through the creation of a new Department of Home Affairs, established formally in December 2017. It was modelled closely on the UK's Home Office but inspired also by the United States' creation of its Department of Homeland Security in 2002.

In 2020 Australia released an even more ambitious Cyber Security Strategy, with notably higher levels of funding and reflecting an even greater sense of urgency.[5] It adopted a much sharper tone around the threats from other countries (which were not named, even though the government had been vocal about banning Huawei from national systems since at least 2012) and highlighted the risks associated with rapidly changing technologies and even higher levels of connectivity. It was clear from this new document that cyber security had moved to the centre stage of Australian government thinking about national security.

The transition between the 2016 and 2020 cyber-security strategies was also evident in the domain of defence policy. The 2016 Defence White Paper made large-scale provision for the expansion of cyber and intelligence capabilities as part of a new strategic orientation around war in the information domain.[6] It repeated one of the fundamental planks of Australian security policy: deepening partnership with the US, especially through higher levels of military integration, inter-operability and intelligence-sharing.[7] This included cyber policy and operations. Cyber threats were identified as one of six key drivers of Australian military strategy.[8] The government assessed that the US would remain the pre-eminent global military power over the next two decades, in large part because of its scientific and industrial capability.

The military also saw organisational reform on cyber that occurred in tandem with the shake-up of the civil sector. On 30 June 2017, the Australian Defence Force (ADF) established a new Information Warfare Division (IWD), commanded at two-star level, which was subordinate to a new Joint Capabilities Group, commanded at three-star level (equivalent in rank in Australia to the chiefs of the single services).

One practical implication of the reforms was that new operational concepts and doctrines needed to be ironed out. This had less of an impact in the civil agencies but even there the changes were significant. In 2018 the government abandoned its commitment to an annual update of the 2016 cyber-security strategy and decided it was no longer fit for purpose. The policy environment had changed significantly with the escalation of threats in cyberspace, including the increasing use of the information domain by Russia and China for political interference, most notably by the Russians in the run-up to the 2016 US presidential election.

**In 2020 Australia released an even more ambitious Cyber Security Strategy**

Australia issued a Defence Strategic Update[9] and a Force Structure Plan[10] in July 2020, followed in August by the new Cyber Security Strategy. All three documents demonstrate heightened concern about threats in cyberspace, continuing commitment to previously announced reforms, and some acceleration of the pace of reforms and spending commitments. In the defence context, Prime Minister Scott Morrison saw new cyber-strike capabilities as an important part of a stiffened posture of credible deterrence.[11] For the first time in such military-policy documents, there was a greater and more urgent emphasis on strengthening information and cyber capabilities than on the traditional categories of land, sea and air. The two defence documents together represent a distinct evolution towards the

view that 'information underpins all effective military operations',[12] even though the government and the ADF continue to shy away from the concept of information dominance as used by the US. A new ADF military doctrine for cyberspace operations was also issued in 2020 but remains classified. It is understood to be essentially an Australian version of the US doctrine on cyberspace operations, with some changes of emphasis reflecting the country's quite different circumstances.

## Governance, command and control

Major decisions on security policy are made by the National Security Committee of Cabinet, with the prime minister acting as de facto commander-in-chief of the armed forces and ultimate authority for all government decisions. This operates in parallel with a system of ministerial responsibility (including for the intelligence agencies) and statutory responsibility for the Chief of the Defence Force in military matters. The National Security Committee of Cabinet sets broad policy, such as approval of new strategies, and the operational priorities of the agencies. The Expenditure Review Committee of Cabinet approves funding plans, sometimes merely endorsing those made by the other committees because of some overlap in membership.

The main cyber-related intelligence agency, the Australian Signals Directorate (ASD), reports directly to the minister for defence, who authorises operations and sets the standards for protecting the privacy of citizens.[13] While therefore under civilian political control, there is also a de facto line of authority flowing from the Chief of the Defence Force, given that ASD includes a large number of military personnel. The personnel strength of ASD is not revealed publicly.

Within the ADF, the IWD has continued to evolve. When it was created in mid-2017, the IWD's most important element was the Joint Cyber Unit, projected to acquire about 1,000 personnel within a ten-year time frame. The ADF announced in January 2018 that the Joint Cyber Unit and a newly created Joint SIGINT Unit, alongside civilian teams from ASD, would operate under a new structure within the IWD, the Defence Signals Intelligence and Cyber Command (DSCC), headed by a one-star officer who had previously led teams in ASD.[14] The aim was to bring 'all ADF SIGINT and cyber personnel working within ASD together in a more refined command structure'.[15]

The DSCC provides a means of unifying ASD's primary responsibility for offensive cyber operations with the clearly competing need for the ADF to share control of that command function. The IWD is not the command authority within the ADF for those operations, since that falls to ASD. The IWD has a role similar to the 'raise, train and sustain' functions of the chiefs of service, who defer to combatant commanders for control of operations.[16]

ASD retains the lead role in civil-sector cyberspace policy, in large part through its subordinate agency, the Australian Cyber Security Centre (ACSC) which manages domestic affairs in this field. In that role, the ACSC and ASD report to the home affairs minister, even though ASD is accountable more directly to the prime minister and the minister for defence. ASD works with the Australian Security Intelligence Organisation (ASIO) on joint cyber operations inside Australia.

## Core cyber-intelligence capabilities

ASD provides the bulk of the country's core cyber-intelligence capabilities, which are closely combined with its cyber-security and cyber-warfare functions. It has strong regional cyber expertise, with a focus on Southeast and East Asia, particularly Indonesia and China. ASD's wider intelligence reach is not so strong but is significantly enhanced through membership of the Five Eyes alliance.

ASD is part of a mature national intelligence community and works in close partnership with the domestic security agency, ASIO, and the external agency, the Australian Secret Intelligence Service, which specialises in overseas human intelligence collection and covert operations. Drawing on the example of the US, Australia created the post of Director of National Intelligence in 2018, to give the government a single source of authority for coordination of the analytical and collection work of all the intelligence agencies, as well as oversight of covert activity.

## Cyber empowerment and dependence

Australia is among the world's leading countries in terms of average internet usage, per capita mobile-broadband

subscriptions and the proportion of companies that are engaged in e-commerce.[17] However, it falls outside the top ten in many other indicators of innovation, competitiveness and cyber security.

Since the turn of the century, Australia's digital economy has mostly stood still in relative terms – for example, its information industries' share of total global value added hardly increased between 2006 and 2016.[18] There is a mismatch between its innovation inputs (knowledge, research and investment), in which it ranked 13th in the world in 2020, and its innovation outputs, in which it ranked only 31st (with a particularly low position, 40th, in the specific area of knowledge outputs).[19] According to the same analysis, the country ranks among the world's top ten in terms of the expertise of its institutions and scientists, and access to venture capital, but performs much less well when it comes to the commercialisation of scientific knowledge.

This mismatch is reflected in the approach to artificial intelligence (AI). For example, Australia was in 11th position in a 2020 ranking of countries according to the number of top-cited AI research papers they produced,[20] yet it lacks the industrial capability to fully exploit this research in economic terms. A 2019 report commissioned by the government estimated that by 2030 the country will need to train at least 32,000 and perhaps as many as 161,000 workers as AI specialists if it is to realise the economic potential of its research strengths.[21] There have been efforts to address this issue – in 2019, for example, the government's main scientific research body published an AI road map and issued a call for public submissions on AI policy – but these initiatives will take many years to bear fruit.[22]

Australia boasts an increasing number of successes in the ICT sector, including in fields such as quantum computing, but research is often funded by US government agencies or US venture capital.[23] That said, the Department of Defence maintains a vigorous and highly regarded Defence Science and Technology Group, which has an active research and development (R&D) programme in cyberspace technologies.[24]

In 2018 the government set up the National Space Agency to help reverse the country's near-total dependence on foreign-owned satellites. It is funded at a modest level – A$9.8 million (US$6.8m) in 2019–20 – and operates 13 satellites.[25] In October 2019 the country joined a small space force with Canada, France, Germany, the UK and the US.

Overall, Australia has a modest capability to assess the security implications of imported technologies, with the best capabilities concentrated largely in government and in several larger corporations. The country contributes significantly to collaborative research both in the commercial and open-source scientific sectors, and in classified work with its closest intelligence and military allies.

## Cyber security and resilience

Successive Australian governments have made important efforts to improve national cyber security and the resilience of the country's critical infrastructure.[26] An education campaign was launched in 2011 around the 'top four' threats to cyber security,[27] based on a list of mitigation strategies advocated by ASD. The four became an 'essential eight' mitigation strategies in 2017, and ASD's full list of 35 strategies was augmented to 38. The programme has been emulated in the UK and Canada. By 2020 the government had significantly improved its cyber-security guidance for all sectors.[28]

**Since the turn of the century, Australia's digital economy has mostly stood still in relative terms**

The state of Australia's national cyber security has been well documented in numerous government statements, several of which have found significant weaknesses in the government's own practices. The Australian National Audit Office has identified considerable recalcitrance on the part of government agencies when it comes to upgrading their cyber security – for example, its 2018 audit of three government agencies revealed that only one was compliant with the ASD top four, which were not even a particularly rigorous set of standards,[29] and in 2019 it found that the Australian postal service had not been able to manage cyber-security risks effectively.[30] In 2020, a parliamentary committee called for more reviews of

cyber security in government departments because of a continuing shortfall in compliance.[31] Nevertheless, Australia was ranked tenth out of 175 in the 2018 Global Cybersecurity Index compiled by the International Telecommunication Union (ITU).[32]

In 2016 the government created a cyber-security 'growth centre' to drive better national performance and reduce the levels of dependence on imported ICT equipment and foreign workers.[33] Now called AustCyber, it provides regular updates on the global competitiveness of the country's cyber-security sector.[34] Its 2019 update, which was notably sober in tone, reported that 'Australian demand and employment is dominated by outsourced cyber security services, and more than three-quarters of this market is controlled by foreign companies', even though these operated mostly 'from local bases and employing Australians'.[35] Such shortcomings are not surprising given that most members of the G20 – including China, France, Germany, Japan, Russia and the UK – also rely very heavily on foreign-made ICT. The document also assessed that 'several hurdles are making it difficult for Australia to fully harness existing advantages and develop a sizeable worldclass cyber security sector'.

The 2019 AustCyber update concluded that Australia needed to address its skills shortage in the cyber-security sector, do better at R&D, improve the business environment for start-ups, improve access to global markets, and develop credible metrics to assess the development of the sector and its economic impacts on the broader economy.[36] To make those steps a reality, the report urged the creation of a more advanced and resilient cyber-security mindset. If such changes are made, many in the policy community see Israel as an exemplar of what Australia could achieve.

The 2016 cyber-security strategy did not have sufficient funding to properly address the problems it identified.[37] One area that needed more attention was digital literacy, especially in tertiary (post-secondary) education – the strategy promised only A$3.5m (US$2.7m) over four years for its main initiative in that area, a programme for academic centres of excellence.[38] AustCyber reported in 2019 that the skills shortage was more severe than initially imagined.[39] By 2020 the government had realised that a cyber-security workforce of the necessary size would not be created without immigration, so it has introduced radical new visa programmes to entice workers from abroad into the field.[40] But Australian universities' response to the new opportunities and demand for cyber-security education could not match the government's ambition, particularly since the government was not prepared to invest sufficient funds. The 2020 Cyber Security Strategy invested more heavily in workforce development, education and community initiatives, providing A$50m (US$35m),[41] but this is unlikely to give universities much incentive because the government prefers community- and business-based solutions.

**Many in the policy community see Israel as an exemplar of what Australia could achieve**

Australia has moved towards a more coherent policy and legislative framework for cyber security and resilience, but the changes need to be reflected in better governmental coordination and more consistent use of standardised tools. The country has not yet made adequate investments to defend against the most serious potential threats.[42] Its providers of critical national infrastructure appear not to have a sufficient understanding of the risks and the situation is aggravated by a shortage of personnel with the relevant skills, including at board level.[43] However, such issues are common to all the countries studied in this report.

## Global leadership in cyberspace affairs

Australia has taken an active role in the management of cyberspace issues within the framework of several international organisations, including the United Nations, ITU, Association of Southeast Asian Nations (ASEAN) and Asia-Pacific Economic Cooperation group. A prime example was its role as co-chair of a working group on cyber security in the ASEAN Plus framework. It has always cooperated closely with its allies in this regard, based on the principle laid out in its 2016 Defence White Paper that, despite having no shortage of resources, it could only deliver national security effectively by working with partners.[44] In 2017, following the example

of other countries such as the US and China, Australia published an International Cyber Engagement Strategy addressing all diplomatic aspects of cyberspace management, including cyber crime, digital trade, cyber security, human rights, privacy and international security.[45] The most innovative part of the strategy was the emerging commitment, shared with its closest allies, to undertake active defence in cyberspace, involving the setting of expectations for state behaviour, practical confidence-building measures and responding to unacceptable behaviour by states.[46] Australia has also participated in the UN Group of Governmental Experts on cyberspace security, including by chairing it from 2013–15.[47]

Australia has been implementing a modest programme of capacity-building for cyber security in Southeast Asia and the South Pacific since 2016. This has probably achieved the greatest impact in partnership with other donor governments, rather than in the projects delivered solely by Australian providers, but the effectiveness of some aspects of the programme is open to question. It is arguably unrealistic to aim to build cyber-security capacity in states with very low levels of economic development in the ICT sector, scarce resources for education and only very few officials in cyberspace-related roles. Countries as poor as Cambodia or Laos, or the microstates of the South Pacific, are less likely to profit from such projects than Indonesia or Vietnam.

The country has aligned more closely than most other US allies with Washington's move to exclude the Chinese company Huawei from national 5G networks, and was in the vanguard of international lobbying to that effect.[48] In August 2018 it became the first Five Eyes member to advise its telecoms operators to avoid purchasing 5G equipment or services from Huawei. This not only soured relations with China but also put Australia at odds with the UK and Canada on the issue for almost two years. The extent to which the decision was the outcome of broader geopolitical concerns, rather than specific technical issues, remains unclear.

Australia has been opposed to China's increasing investment in the ICT sectors of regional countries, especially in the South Pacific – a position demonstrated most strikingly in 2018 when it successfully pressured the Solomon Islands to abandon a deal with Huawei for an undersea cable to Australia in favour of a deal that excluded all Chinese companies.[49] It has not had similar success with Papua New Guinea, which is reliant on Australian aid but determined to resist pressure to abandon Huawei.[50]

The country conducts bilateral and multilateral dialogues on cyberspace affairs, including with Canada, China, India, Indonesia, Japan, New Zealand, South Korea, the UK and the US. The US–Japan–Australia trilateral dialogue is particularly important as a way for Canberra to signal its positions on internet freedom and malign behaviour by states.

## Offensive cyber capability

In 2016 Australia officially avowed that it possessed an offensive cyber capability and had used it against the Islamic State (also known as ISIS or ISIL).[51] The head of ASD confirmed in 2019 that those operations had been conducted jointly with coalition partners and that the Australian dimension, under the direction of the ADF's Chief of Joint Operations, involved both the degrading of Islamic State battlefield communications and an online influence operation.[52] He added that the country's capabilities would also be directed at 'organised offshore cyber criminals'.[53] Australia has also provided support to the US Cyber Deterrence Initiative, which involves public attribution of foreign attacks and engagement in cyberspace to disrupt them. Australian offensive cyber operations are conducted in accordance with the country's understanding of international law and are closely scrutinised by a growing number of government lawyers specialising in the field.

In its five-year corporate plan published in 2019, ASD reiterated its mission on offensive cyber operations, linking it to domestic requirements (countering cyber crime) as well as to warfighting needs.[54] The plan aimed to build a world-class offensive cyber capability[55] while emphasising that ASD's ability to conduct operations would be underpinned by its close international partnerships.[56]

Overall, Australia has effective offensive cyber capabilities. Its close partnership and joint operations with the US and the UK secure its place in the front rank of states in terms of offensive cyber, while its membership of the Five Eyes alliance provides it with the enhanced intelligence and situational awareness needed for

top-end operations. At the same time, in terms of resources and available personnel, Australia does not match the capabilities of its senior allies.

In common with all other states, the biggest constraint on Australia's offensive cyber capability may well be the limited extent of its national skills base and pipeline. ASD official documents regularly allude to this challenge, and many of its public statements, including revelations of offensive cyber operations, are accompanied by recruitment appeals.

## Notes

1 Australian Government, Attorney-General's Department, 'Cyber Security Strategy', Canberra, November 2009, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/AGCyberSecurityStrategyforwebsite.pdf.

2 See Gary Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure', in Greg Austin (ed.), *National Cyber Emergencies: The Return to Civil Defence* (Abingdon: Routledge, 2020), pp. 93–105.

3 Australian Government, Department of the Prime Minister and Cabinet, 'Australia's Cyber Security Strategy: Enabling Innovation, Growth and Prosperity', Canberra, 2016, https://www.homeaffairs.gov.au/cyber-security-subsite/files/PMC-Cyber-Strategy.pdf.

4 *Ibid*., p. 6.

5 Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy', Canberra, August 2020, https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf.

6 Australian Government, Department of Defence, '2016 Defence White Paper', Canberra, 2016, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf.

7 *Ibid*., p. 35.

8 *Ibid*., p. 41.

9 Australian Government, Department of Defence, '2020 Defence Strategic Update', Canberra, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Defence_Strategic_Update.pdf.

10 Australian Government, Department of Defence, '2020 Force Structure Plan', Canberra, July 2020, https://www.defence.gov.au/StrategicUpdate-2020/docs/2020_Force_Structure_Plan.pdf.

11 Australian Government, Prime Minister of Australia, 'Address – Launch of the 2020 Defence Strategic Update', Canberra, 1 July 2020, https://www.pm.gov.au/media/address-launch-2020-defence-strategic-update.

12 *Ibid*., p. 36.

13 Australian Government, Australian Signals Directorate, 'Accountability', https://www.asd.gov.au/accountability.

14 Australian Government, Department of Defence, 'Defence Chief Announces New Command', Canberra, 30 January 2018, https://news.defence.gov.au/media/media-releases/defence-chief-announces-new-command.

15 *Ibid*.

16 This is explained by IWD as follows: 'IWD is developing the information warfare capabilities for the ADF to employ in all its activities, such as protecting its networks and missions systems, conducting exercises and training events, supporting the community and our region in disaster relief, stability and security operations through to full conflict and war. The capabilities IWD develops are put into operation by the ADF. Chief of Joint Operations [*sic*] is responsible for how the capabilities are used to meet the directions of the Australian Government.'

17 See International Telecommunication Union, 'Statistics', https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx; and Organisation for Economic Co-operation and Development (OECD), 'Measuring the Digital Transformation: A roadmap for the future', 11 March 2019, pp. 54, 101, 121, https://www.oecd.org/publications/measuring-the-digital-transformation-9789264311992-en.htm.

18 OECD, 'Measuring the Digital Transformation: A roadmap for the future', p. 71.

19 SC Johnson College of Business Cornell University, INSEAD and the World Intellectual Property Organisation, *Global Innovation Index 2020: Who Will Finance Innovation*?, 2020, pp. xxxiv, xxxvi, 15, https://www.globalinnovationindex.org/Home.

20 Gleb Chuvpilo, 'AI Research Rankings 2020: Can the United States Stay Ahead of China?', 21 December 2020, https://chuvpilo.medium.com/ai-research-rankings-2020-can-the-united-states-stay-ahead-of-china-61cf14b1216.

21 Australian Government, 'Artificial Intelligence: Solving problems, growing the economy and improving our

quality of life', 2019, p. iv, https://data61.csiro.au/~/media/D61/AI-Roadmap-assets/19-00346_DATA61_REPORT_AI-Roadmap_WEB_191111.pdf?la=en&hash=58386288921D9C21EC8C4861CDFD863F1FBCD457.

22 For an overview of Australian AI policy, see the OECD AI Observatory, https://oecd.ai/dashboards/countries/Australia.

23 See, for example, the case of quantum computing at the University of Sydney, as reported in 'Global VC Bets on Australian Quantum Computing Start-Up Q-Ctrl in Us$15m Series A', Quantaneo, 10 September 2019, https://www.quantaneo.com/Global-VC-bets-on-Australian-quantum-computing-start-up-Q-CTRL-in-US15m-Series-A_a205.html; and IARPA, 'US investing in quantum tech at Sydney University', Technology Decisions, 9 May 2016, https://www.technologydecisions.com.au/content/it-management/article/us-investing-in-quantum-tech-at-sydney-uni-672014055.

24 Australian Government, Department of Defence, 'Defence Science and Technology Group', https://www.dst.defence.gov.au/division/cyber-and-electronic-warfare-division.

25 Union of Concerned Scientists, 'UCS Satellite Database', updated 1 January 2021, https://www.ucsusa.org/resources/satellite-database.

26 See Waters, 'National Cyber Emergency Policy for Australia: Critical Infrastructure'.

27 For a discussion, see Stilgherrian, 'Australia's cyber defence "pretty ordinary" before ASD's Top Four', ZDNet, 2 June 2015, https://www.zdnet.com/article/australias-cyber-defence-pretty-ordinary-before-asds-top-four.

28 See, for example, the Australian Government Information Security Manual (ISM), which 'assists in the protection of information that is processed, stored or communicated by organisations' systems'. Australian Government, Australian Signals Directorate, 'Australian Government Information Security Manual', September 2019, https://www.cyber.gov.au/ism; Australian Government, Australian Signals Directorate, 'Strategies to Mitigate Cyber Security Incidents' (which complements the advice in the ISM), February 2017, https://www.cyber.gov.au/publications/strategies-to-mitigate-cyber-security-incidents; and Australian Government, Australian Signals Directorate, 'The Essential Eight Maturity Model', 26 June 2020, https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-maturity-model.

29 Australian National Audit Office, 'Cyber Resilience', Auditor General Report, no. 53 of 2017–18, 28 June 2018, https://www.anao.gov.au/work/performance-audit/cyber-resilience-2017-18.

30 Australian National Audit Office, 'Cyber Resilience of Government Business Enterprises and Corporate Commonwealth Entities', Auditor General Report, no. 1 of 2019–20, 4 July 2019, https://www.anao.gov.au/work/performance-audit/cyber-resilience-government-business-enterprises-and-corporate-commonwealth-entities.

31 Joint Committee on Public Audit and Accounts, 'Report 485 Cyber Resilience', December 2020, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Public_Accounts_and_Audit/CyberResilience2019-20/Report.

32 International Telecommunication Union, 'Global Cybersecurity Index 2018', p. 58, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

33 The goals of the growth-centres initiative in the designated sector are to increase collaboration and commercialisation; to improve international opportunities and market access; to enhance management and workforce skills; and to identify opportunities for regulatory reform. See Australian Government, Department of Industry, Science, Energy and Resources, 'Industry Growth Centres', https://www.industry.gov.au/strategies-for-the-future/industry-growth-centres.

34 AustCyber, 'Australia's Cyber Security Sector Competitiveness Plan–2019Update', December 2019, https://www.austcyber.com/resource/australias-cyber-security-sector-competitiveness-plan-2019.

35 *Ibid.*, p. 33.

36 *Ibid.*, p. 10.

37 Abbey Dorian, 'Meeting Australia's Cyber Security Challenge', Australian Institute of International Affairs, 17 October 2019, http://www.internationalaffairs.org.au/australianoutlook/meeting-australias-cyber-security-challenge.

38 Australian Government, 'Portfolio budget statements 2016–17: Budget related paper no. 1.5: Education and Training Portfolio', pp. 14, 20, https://www.dese.gov.au/download/3174/education-and-training-portfolio-budget-statements-2016-17-full-version/18354/document/pdf.

39 AustCyber, 'Cyber Security Competitiveness Plan – 2019 Update', p. 11.

40 It took Australia several years to set its immigration policies in a way that would attract higher numbers of cyber-security professionals. The government started in 2017 with the overarching Global Talent Employer Sponsored (GTES) programme, which aimed to find talent for 'highly-skilled niche positions' (without specifying cyber security) that could not be filled by Australians or through other visa programmes

such as those for short-term and medium-term skilled temporary residents. This was followed in 2018 by a scheme that focused on seven 'future-focused fields', including cyber security, but employer sponsorship was still required – the aim was to recruit 5,000 immigrants in the scheme's first year of operation. In November 2019, the government launched a new programme for skilled migration that would allow applications from individuals, not just from the sponsoring employer. See Greg Austin, 'Twelve Dilemmas of Reform in Cyber Security Education', in Greg Austin (ed.), *Cyber Security Education: Principles and Policies* (Abingdon: Routledge, 2020), pp. 208–21.

41 Australian Government, Department of Home Affairs, 'Australia's Cyber Security Strategy 2020', p. 42.

42 'Australia Needs Civil Defence against the Cyber Storm: Policy Report', Research Group on Cyber War and Peace UNSW, University of New South Wales Canberra, 31 March 2019, p. 3, https://www.unsw.adfa.edu.au/unsw-canberra-cyber/sites/accs/files/uploads/Policy%20Report%20Cyber%20Civil%20Defence%2031%20March%202019_1.pdf.

43 Rajiv Shah, 'Protecting critical national infrastructure in an era of IT and OT convergence', Australian Strategic Policy Institute, Policy Brief, no. 18/2019, 12 July 2019, https://www.aspi.org.au/report/protecting-critical-national-infrastructure-era-it-and-ot-convergence.

44 Australian Government, Department of Defence, '2016 Defence White Paper', Canberra, 2016, p. 45, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf. 'While Australia is the world's twelfth largest economy and has sophisticated and growing military capabilities, Australia does not have the capacity to unilaterally protect and further our global security interests. This means we will be working with our alliance partner the United States, ASEAN countries, the North Atlantic Treaty Organisation (NATO), the United Nations and other partners to achieve our common goals in protecting and promoting a stable rules-based global order.'

45 See Australian Government, Department of Foreign Affairs and Trade, 'Australia's International Cyber Engagement Strategy', October 2017, https://www.dfat.gov.au/international-relations/themes/cyber-affairs/Pages/australias-international-cyber-engagement-strategy.

46 *Ibid*., p. 44.

47 Since a UN General Assembly resolution in 2004, a UN Group of Governmental Experts (GGE) has convened for two-year terms to address international-security aspects of cyberspace. It was known as the GGE on 'Developments in the Field of Information and Telecommunications in the Context of International Security' until 2018, when it was renamed the GGE on 'Advancing Responsible State Behaviour in Cyberspace in the Context of International Security'. In cyberspace-policy circles it is common to refer to it simply as 'the GGE'. See UN Office for Disarmament Affairs, 'Developments in the field of information and telecommunications in the context of international security', https://www.un.org/disarmament/ict-security.

48 See 'Australia, Huawei and 5G', IISS *Strategic Comments*, vol. 25, no. 28, October 2019, https://www.iiss.org/publications/strategic-comments/2019/australia-huawei-and-5g.

49 Rosie Perper, 'Australia snubbed Huawei and completed its undersea cable project to bring high-speed internet to Pacific Islands', Business Insider, 28 August 2019, https://www.businessinsider.com.au/australia-snubs-huawei-finishes-undersea-cables-for-pacific-islands-2019-8?r=US&IR=T.

50 Alan Burkitt-Gray, 'Australia slams Huawei for "security vulnerabilities" in PNG data centre', Capacity Media, 12 August 2020, https://www.capacitymedia.com/articles/3826128/australia-slams-huawei-for-security-vulnerabilities-in-png-data-centre.

51 Parliament of Australia, 'National Security Update on Counter Terrorism: Address to the House of Representatives, Parliament House, Canberra', 23 November 2016, https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22media/pressrel/4951827%22.

52 Australian Signals Directorate, 'Director-General ASD speech to the Lowy Institute', 27 March 2019, https://www.asd.gov.au/publications/speech-lowy-institute-speech.

53 *Ibid*.

54 On warfighting, the plan says: 'ASD supports Australian Defence Force (ADF) operations around the globe, including by providing intelligence and offensive cyber capabilities to enable the warfighter and protect ADF personnel and assets'. Australian Government, Australian Signals Directorate, 'ASD Corporate Plan 2019–20', Canberra, 2019, p. 7, https://www.asd.gov.au/sites/default/files/2019-08/ASD_Corporate_Plan_final_12.pdf. The title is a little misleading, however, as the document actually covers the period 2019–23.

55 *Ibid*., p. 8.

56 *Ibid*., p. 13.