In this section CyAN makes observations which we see as central to any consideration of Australia’s cybersecurity strategy.

1. **The purpose and objectives of Australia’s Cyber Security Strategy**

Australia’s 2016 Cybersecurity Strategy[[1]](#footnote-1) provided a much needed response to the rapidly escalating ongline threats facing Australian governments, business and society. It set out an initial set of actions grouped into five broad themes:

1. **A national cyber partnership** – to strengthen the governance of cybersecurity policy
2. **Strong cyber defences** – to strengthen public private partnerships in cyber defence activities
3. **Global responsibility and influence** – to strengthen international cooperation in cybersecurity policy and operations – particularly against transnational criminal organisations
4. **Growth and innovation** – to foster indigenous research and innovation, and the development of the cybersecurity industry
5. **A cyber smart nation** – to improve cybersecurity awareness and develop the cybersecurity workforce

The scope of these actions were necessarily focussed on establishing the institutional foundations for a national cybersecurity capability, as the Government recognised that “both Government and the private sector have vital roles to play”.

Much progress has been made, particularly in strengthening collaboration between federal government agencies and critical national infrastructure operators. Some of the major institutional reforms have included:

* The establishment of the Australian Signals Directorate as a statutory agency within the federal government with responsibility for the Australian Cybersecurity Centre, the national Computer Emergency Response Team, incident monitoring and response, and the Cybersecurity Unit
* Promoting the adoption of baseline cybersecurity controls in federal government agencies, including the role of the Australian National Audit Office in identifying cybersecurity risks and promoting the implementation of appropriate controls[[2]](#footnote-2)
* Strengthening regulatory and operational collaboration getween the federal government and critical national infrastructure industries, particularly through sector-specific initiatives such as the Telecommunications Sector Security Reforms

The question is whether the Government’s current cybersecurity framework is able to be extended to support the rest of society. There is a lot of work remaining to be done to extend the scope of our cybersecurity defences to state and local government, across the private sector, and civil society. Our definition of critical national infrastructure needs to be expended to include an increasing range of sectors including health care, education, and the media. As the focus moves into these increasingly diverse and fragmented sectors of the economy, we need to find more scaleable, flexible and cost effective models for the provision of cybersecurity services that are attuned to the needs of specific industries or sectors of society.

1. **Measuring the success and efficiency of Australia’s cybersecurity activities**

The second iteration of Australia’s cybersecurity strategy provides an opportunity to tighten the coordination and control of the activities within its scope. The 2016 Cybersecurity Strategy allocated $230m “*to enhance Australia’s cybersecurity capability and deliver new initiatives, complementing the significant investment in cyber security outlined in the 2016 Defence White Paper*”[[3]](#footnote-3). Federal government funding for cybersecurity is fragmented across multiple agencies including the Department of Home Affairs, Foreign Affairs and Trade, Health and Industry Science and Technology, as well as Defence. Additional cross-portfolio measures are contained in two cross-portfolio packages—‘Delivering Australia’s Digital Future’ and ‘Australian Technology and Science Growth Plan’. This situation makes it difficult to consolidate and track the progress of cybersecurity initiatives at a holistic level.

The Parliamentary Library’s 2018 budget review noted that:

 *“There is… no explicit detail in the Budget on how any particular measure ties in with the Strategy, or the specific outcomes being sought in cyber policy… While the 2016 Cyber Security Strategy and the more recently announced*[*International Cyber Engagement Strategy*](http://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf)*may aim to coordinate this policy intersection inside government, a coherent conception of cyber policy remains absent in broader public discourse and in parliamentary debates.”[[4]](#footnote-4)*

The Europen Union Agency for Cybersecurity (ENISA) has begun to address similar concerns by developing an evaluation framework for national cybersecurity strategies and other practice guides for strengthening and continuous enhancement of cybersecurity frameworks[[5]](#footnote-5). Australia should consider whether adopting a similar approach may assist in the governance and management of a mature sustainable, cybersecurity policy.

1. **Cyber policy as an enabler of a vibrant ICT and knowledge economy**

It is trite to observe that our economy is becoming increasingly reliant on information and communications technology (ICT). Of concern is mounting evidence that Australia is falling behind other members of the OECD in the contribution that our ICT sector makes to our financial prosperity.[[6]](#footnote-6) Cyber policy is clearly an enabler of ICT and an effective cyber strategy is a pre-condition to a productive and profitable ICT sector. Put another way, growing our ICT sector to deliver the contribution to national wealth that all Australians should expect will be very difficult without a coherent and effective cybersecurity strategy. There are many lenses through which to view cybersecurity policy but CyAN sees this lens, the emphasis on fostering a knowledge economy, as the most important.

We also believe that the very same factors that have led to growth in the ICT sectors of the most successful nations must be considered when developing a cybersecurity strategy. In particular we emphasise the importance of Government fostering collaboration between Government, academia and business.

1. **Growing Australia’s cyber capability through partnerships with academia and industry**

CyAN acknowledges that the actions identified in Appendix A to the Discussion Paper (particularly actions 27 – 31) evidence good progress at fostering collaboration but as a cybersecurity industry body, CyAN sees tremendous opportunity for more and better collaboration between Government, academia and industry.

The Cyrise cybersecurity incubator[[7]](#footnote-7) is an example of industry and academia partnering (with the assistance of Government) and shows that Australian institutions can foster innovation in ways that mirror the Silicon Valley experience. The challenge in Australia for startups tends to be finding markets of sufficient size to permit commercial viability. Austrade has done some good work taking Australia business to offshore markets and CyAN would support Austrade focussing on cybersecurity business models or developing programmes designed specifically for cybersecurity offerings.

Another means of fostering partnerships and collaboration between governemnet and industry is through the sourcing of public infrastructure solutions from the private sector. CyAN sees the potential for development of national security infrastructure being delivered under PPP type models. In the Discussion Paper (p. 9) there is reference to Government potentially playing a role in protecting businesses from malicious ations. CyAN envisages such public cybersecurity infrastrucrure being delivered using industry expertise under partnership models. The benefit of this approach is delivery of essential cybersecurity infrastructure at the same times as promoting cybersecurity industry expertise.

1. Commonwealth of Australia Department of the Prime Minister and Cabinet, Australia’s Cybersecurity Strategy, 2016 [↑](#footnote-ref-1)
2. Commonwealth of Australia Australian National Audit Office, Review of Cyber Security: Report by the Independent Auditor, December 2017 [↑](#footnote-ref-2)
3. Commonwealth of Australia Department of the Prime Minister and Cabinet, Australia’s Cybersecurity Strategy, 2016, p.3 [↑](#footnote-ref-3)
4. Commonwealth of Australia Department of Parliamentary Services, Budget Review 2018-19, 23rd May 2018, https://parlinfo.aph.gov.au/parlInfo/download/library/prspub/5982057/upload\_binary/5982057.pdf [↑](#footnote-ref-4)
5. European Union Agency for Cybersecurity, Evaluation framework for Cyber Security Strategies, November 27, 2014, https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies [↑](#footnote-ref-5)
6. “Growing Australia’s technology sector at the same rate as countries like the US, UK, France and Japan would add $40-$50 billion per year in GDP over the next 20 years, boosting GDP by 1.2-1.5%. Based on our analysis of global technology leaders, we make six recommendations:

	1. Foster collaboration between government, academia and business
	2. Incentivise research, development and innovation
	3. Encourage greater investment in technology and innovation
	4. Ensure policies and regulations are pragmatic and globally consistent
	5. Skill the workforce of the future
	6. Improve access to global talent”See “Australia’s Digital Opportunity” Alpha Beta, September 2019 <https://www.alphabeta.com/our-research/australias-digital-opportunity-growing-a-122-billion-a-year-tech-industry/> [↑](#footnote-ref-6)
7. <https://www.cyrise.co/about.html> [↑](#footnote-ref-7)