Innovate UK
KTN

PUBLIC

Global Expert Mission
Australia – Cybersecurity 2022

Contents

Executive Summary

In October 2022, an Innovate UK Global Expert Mission visited Australia (Canberra, Melbourne and Sydney) to gain a more in-depth understanding of the cybersecurity ecosystem and identify opportunities for collaboration.

The UK delegation consisted of representatives from Innovate UK, the UK government, academia and industry. They met with representatives in Australia from the government (federal and state), academia, innovation hubs, accelerators and companies.

The mission gave the delegates a greater understanding of the innovation landscape in Australia in the cybersecurity sector and how it differs from its counterpart in the UK.

Australia has a young but growing cybersecurity ecosystem supported by government funding and direct initiatives to support its growth both by the federal and state governments. Most of the activity is focused on four states/territories, and the ecosystems primarily focus on the main local markets. These ecosystems are well coordinated through state-led support. The private investment landscape is patchy, with start-ups having to look to the US and, regionally, to Singapore to raise funding.

Australia also recognises the global opportunity, and they have a well-defined international engagement strategy alongside initiatives like the Landing Pads programme designed to accelerate growth in the sector and position Australia at the heart of global activity in the cybersecurity area. The United Kingdom and Australia maintain a long-standing partnership in the realm of defence and security, including being members of the Five Eyes, Five Power Defence Arrangements and most recently, AUKUS.

AUKUS is a trilateral security pact between Australia, the United Kingdom, and the US, announced on 15 September 2021 for the Indo-Pacific region. Under the pact, the US and the UK will help Australia to acquire nuclear-powered submarines. The pact also includes cooperation on advanced cyber, artificial intelligence and autonomy, quantum technologies, undersea capabilities, hypersonic and counter-hypersonic, electronic warfare, innovation and information sharing.

Additionally, the recent free trade agreement[1] between the two countries provides further impetus to build closer ties. Moreover, the British and Australian governments share similar interests and perspectives on international matters and relatively close political links. According to the Australian Department of Foreign Affairs and Trade, the UK traditionally holds the position as Australia's second biggest foreign investor, only behind the US and considerably ahead of its competitors such as Belgium, Japan, China and Germany.[2]

The UK is seen as one of the world's leading hubs for cybersecurity and innovation. The regulatory regime is also more advanced in the UK than in many other countries. Australia looks to the UK and the US on aspects of regulation, standards and best practice when making its own policy decisions.

Skills shortages are seen as a significant barrier to innovation and growth in both the UK and Australia. Australia has several initiatives underway to try to foster more home-grown capability in cybersecurity and digital technologies more generally.

The mission highlighted a number of opportunities for closer collaboration between the two countries. The key opportunities were focused around closer harmonisation of regulation and standards to enhance trade and collaboration on critical technologies, securing supply chains, cyber skills certification, bilateral collaboration on innovation around securing critical technologies, IoT security and online safety.

Acronyms and Definitions

DCMS	Department of Digital, Culture, Media and Sports
DfE	Department for Education
DIT	Department of International Trade
DLUHC	Department of Levelling Up, Housing and Communities
DSbD	Digital Security by Design
Dstl	Defence, Science and Technology Laboratory
FCDO	Foreign, Commonwealth and Development Office
GBIP	Global Business Innovation Programme
GIP	Global Incubator Programme
STEM	Science, Technology, Engineering and Mathematics

1. Introduction

The UK cybersecurity market is worth £10.1 billion.[3] It is expected to grow at a CAGR of 11.45% from 2022 to 2027. A rise in cyberattacks, the growing demand for digital technologies, increasing third-party vendor risks in complex supply chains and the growing adoption of cloud-based services have all driven and continue to drive growth in the sector in the UK.

- In December 2021, the British government launched a new National Cyber Strategy[4], which is seen as a "blueprint" to protect the UK from cyber threats and "solidify its position as a global cyber power." The strategy also signals a drive to reduce the UK's reliance on international suppliers or technologies that do not share the UK's values.
- With the growing 5G and full-fibre broadband networks in the country, the government, in collaboration with telecommunication companies, is taking initiatives to improve network security, supply chain resilience, reduce risks from cyberattacks and improve security standards and practices across the United Kingdom's telecoms sector.
- UKRI has funded a number of programmes to support innovation in secure technologies. In 2019, UKRI launched a five-year cybersecurity programme, Digital Security by Design (DSbD). The programme will work with industry and academia to create technology capable of preventing the exploitation of 70% of ongoing vulnerabilities and the potential to mitigate and reduce the impact against new classes of vulnerabilities. DSbD has seen research from the University of Cambridge prototyped in the Arm Morello system-on-chip and development board. The Morello hardware board is available for businesses to access the new technology, increasing their understanding of DSbD technologies, expanding the ecosystem and how it can benefit their business and customers if it becomes commercially available.
- Further, the vulnerability and exposure to diverse cyberattacks have increased with the increasing use and deployment of Internet of Things (IoT) devices. UKRI has been investing in new technologies to increase the security and resilience of IoT systems across industry sectors, through the multidisciplinary programme Security of Digital Technologies at the Periphery (SDTaP).

Innovate UK has led global expert missions to a number of the world's leading cybersecurity innovation hubs (US, Israel and Singapore). Australia's fast-growing cybersecurity ecosystem is seen as one of the main launchpads for servicing a growing market in the Indo-Pacific and ASEAN regions. Australia and the UK have a long shared history, and more recently, the free-trade agreement between the two countries, AUKUS and the Cyber and Critical Technologies Partnership signed in January 2022 between the UK and Australia all provide a basis for closer collaboration and long-term strategic cooperation.[5] Furthermore, Australia shares the belief that there is a need to reduce the reliance on international suppliers from countries who do not share their values for critical technologies and capabilities.

2. Cybersecurity Landscape in Australia

Australia has the ambition to become a globally competitive cybersecurity centre. The Australian cybersecurity market was valued at US$4.6 billion in 2021 and will grow to US$5.8 billion by 2024.[6] The market is growing by over 8% annually, and the Australian Cyber Security Growth Network (AustCyber)[7] suggests that over the next ten years, the sector has the potential to treble in size.

The federal government sees cybersecurity as one of six industry sectors crucial to the long-term growth of the Australian economy. The sector's revenue has grown by A$800 million since 2017, to reach an estimated A$3.6 billion by the end of 2020.

The UK delegation met with representatives from the following four states where the majority of activity is primarily focused: New South Wales, Victoria, the Australian Capital Territory and South Australia. Western Australia also has an ecosystem focused around the primary industries in the region.

2.1 New South Wales (NSW)

Cybersecurity companies in New South Wales (NSW) primarily focus on the financial services sector, although there has been recent interest from start-ups in advanced manufacturing and automation (Industry 4.0). Atlassian, Secure Code Warrior, Huntsman Security and Kasada represent some of the more high-profile entrants to the market from NSW.[8]

The start-up community appears to be a vibrant one supported by existing and new programmes. These include:

- NSW Cyber Hub providing a range of industry support [9].
- NSW Cyber Business Exchange Programme designed to help established cybersecurity businesses in NSW to grow[10].
- NSW Accelerator in Residence Programme[11].
- NSW Cyber Ambassador Programme[12].

The NSW government published the latest Cyber Security Strategy in 2021[13] with the ambition to

become a world leader in cybersecurity. To deliver on this ambition, the focus is on the following four activities:

1. To lead by example in best practice and cyber resilience.
2. To be progressive and proactive to allow the cyber workforce to expand.
3. To seek opportunities to grow cyber industry commercialisation.
4. To provide practical support to reduce barriers to business growth.

The university sector is also active in research and collaboration with industrial partners in the state. Undergraduate and postgraduate degrees are offered in cybersecurity. The University of New South Wales[14], the University of Technology Sydney[15] and Macquarie University[16] all offer degrees in cybersecurity and have ongoing research programmes in the area.

New South Wales (NSW) Department of Enterprise and Trade/Investment NSW[17]

Investment NSW primarily seeks to grow the local economy and attract foreign direct investment by:

- Enhancing and accelerating research and development.
- Growing and supporting the local start-up ecosystem and emerging innovations.
- Providing the necessary support to bring growth in priority sectors and precincts.
- Attracting global investment and talent.
- Growing export opportunities across the world.

The NSW Cyber Security Strategy of 2021 sets out a vision for NSW to become a world leader in cybersecurity. To achieve this, they look to pursue the following priorities[18]:

- Lead in the adoption of standards and best practice and aim to exceed that.
- Grow the cybersecurity workforce through proactive and progressive policies.
- Increase the opportunities for innovation and commercialisation.
- Provide the required support for growth and expansion for local cybersecurity companies and the sector as a whole.

There are more than 200 cybersecurity companies in NSW, and 40% of the national workforce is located in the state.

The NSW Future Economy Fund[19], worth A$703.4 million in 2022-23, is targeted at high-growth businesses in priority sectors with the aim of driving productivity growth in emerging industries and technologies. The fund includes the following earmarked spending:

- A$142 million for research and development (R&D) in areas where NSW has a competitive edge and to further enable collaboration between the regional universities, research institutes and the private sector.
- A$342 million to support the commercialisation of innovative new products and services with targeted support to research institutes, start-ups and small and medium-sized enterprises in NSW.
- A$219 million for accelerating growth and investment in priority sectors such as advanced manufacturing, medtech, defence and aerospace.

The NSW government has a A$3.3 billion Regional Growth Fund[20] (now in its fifth year) aimed at improving local and regional services, activating economic growth, and responding to emerging regional needs. It has also supported numerous private sector–university collaborations.

2.2 Victoria

Victoria has a vibrant cybersecurity start-up scene, and is the home of CyRise[21], Asia Pacific's only dedicated cybersecurity accelerator. Financial services and defence appear to be the two most dominant sectors that companies target. Victoria hosts approximately 145 leading national and multinational digital and cybersecurity businesses and institutions. It is also the location for a number of centralised clusters of cybersecurity innovation hubs and R&D centres of excellence.

The universities in the state actively work closely with industry, government and the research community, and they are responsible for creating a pool of skilled, work-ready graduates. Other tertiary institutions in the state offer more than 200 cybersecurity courses and partnerships with local businesses and government, meaning that the courses are often focused on areas that are directly relevant to a sector.[22]

Invest Victoria[23]

Invest Victoria is a state government agency tasked with attracting foreign direct investment and other investment opportunities. Furthermore, it seeks to enhance the investment environment to make it more attractive and provide the necessary support and incentives.

The demand for cybersecurity is strong in the state of Victoria. It has a large financial sector which contributes 11% of the overall GDP of the state.[24] Within that, Melbourne is the leading city in the country for institutions in pensions and asset management. Alongside this is a strong defence industry dominated by British multinational BAE and French multinational Thales. The state is experiencing rapid growth, and the population is expected to rise from five to eight million within the next 25 years.

There are 150 cybersecurity companies in the state, mostly operating in Melbourne. This is complemented by a strong talent pool which gives them an edge over the regional competition from Hong Kong and Singapore. They are having some success in attracting overseas companies to locate in Melbourne and are actively pursuing that growth agenda. To this end, they have representatives overseas including in London in the UK.

Breakthrough Victoria Fund[25]

The Breakthrough Victoria Fund is an initiative to drive investment in translational research, innovation and commercialisation outcomes to accelerate growth in key industry sectors and create jobs.
The Victoria government launched the A$2 billion fund, which will be managed by a new company, Breakthrough Victoria Pty Ltd[26]. The aim is to also generate further significant investment from other industry, university and government sources with an expectation to create 15,700 jobs over ten years. The fund is focused on health and life sciences, agrifood, advanced manufacturing, clean economy and digital technologies. The fund will support research and development adoption and commercialisation outcomes, prioritising projects with strong commercial potential to accelerate productivity, grow exports, support domestic manufacturing and create jobs.

2.3 The Australian Capital Territory (ACT)

As a proportion of the population, the Australian Capital Territory (ACT) has the largest number of people working in the cybersecurity sector. There is a strong start-up community, mainly targeting government agencies and the defence sector. The cybersecurity start-up community is primarily supported by the Canberra Cyber Hub[27] and the Canberra Innovation Network.

There is considerable activity in the education and research area. ACT hosts the Australian Centre for Cyber Security at UNSW Canberra, and the College of Engineering and Computer Science and National Security College at the ANU. Alongside this, it is also the location for AustCyber's national office and the Canberra Cyber Network - a partnership between ANU, UNSW Canberra, Data61, the University of Canberra and the Canberra Institute of Technology.[28]

Canberra is home to the Australian Signals Directorate (ASD)[29], the Australian counterpart to the Government Communications Headquarters (GCHQ) in the UK. The Australian Cyber Security Centre[30] (ACSC) is the equivalent of the National Cyber Security Centre (NCSC) in the UK and is also hosted within the ASD in Canberra. The ACSC is a hub for private and public sector collaboration and information-sharing on cybersecurity, to prevent and combat threats and minimise harm to Australians.

2.4 South Australia

South Australia has a disparate sector landscape; however, it is dominated by the defence and space sectors. The National Space Centre is headquartered in Adelaide. Adelaide also hosts the South Australian Space Industry Centre (SASIC) which focuses on growing the local space industry, building on South Australia's strong history of space activity. SASIC aims to provide the support that entrepreneurs require to grow their companies and to accelerate innovation through an incubator.[31]

South Australia, relative to NSW, Victoria and ACT, has quite a small pool of cybersecurity companies. It is, however, the base for some of the oldest home-grown cybersecurity companies in Australia. It is the main base for established providers like Prophecy International and Consunet (operating for 28 and 18 years, respectively). Alongside this, there is a small number of younger companies like Airlock Digital and CyberOps.

The development of Lot Fourteen[32] in the state, enhances opportunities for cybersecurity companies to get involved in emerging areas such as machine learning and the space industry. This is seen as something that will add to the state's expertise in the defence sector and potentially present export opportunities.[33]

Lot Fourteen is an initiative to create an area within the city focused on innovation, entrepreneurship, research, education, culture and tourism with a view to growing high-skilled jobs and the local economy. Lot Fourteen is not dissimilar to Tech Central in Sydney, which is covered later in this report.

South Australia is also home to the Australia Cyber Collaboration Centre[34], established in 2020. The centre hosts the largest Cyber Range in the Asia-Pacific. The state government has invested A$10 million in the development of this centre, which will provide support to cybersecurity companies specifically to launch new products and services globally.

Flinders University in the state hosts the Jeff Bleich Centre for the US Alliance in Digital Technology, Security and Governance. The focus is on research into issues such as foreign interference in democratic elections and national security.[35]

There is a dedicated cyber curriculum across high schools, with the ambition for a nationwide rollout. Furthermore, there is a plan to create an academy to build a sustainable skills pipeline.

There is a recognition here as well that harmonisation of regulatory frameworks would ease exports and trade in areas of critical technology and that the recent trade agreement between the two countries and AUKUS are both opportunities to leverage these sorts of initiatives.

2.5 Western Australia (WA)

Four of Western Australia's five universities run cybersecurity courses and provide test bed environments for the development of cybersecurity applications and solutions. Western Australia's Edith Cowan University (ECU)[36] is one of only two universities recognised by the federal government as an Academic Centre of Cyber Security Excellence.[37]

ECU is host to the WA AustCyber Innovation Hub[38], which has the remit to harness and accelerate cyber capability development, innovation and commercialisation across the three domains of critical infrastructure, cybercrime and big data. The hub has collaborated with the Western Australian government, ECU, the national Industry Growth Centre[39], AustCyber and the City of Joondalup. The ECU Security Research Institute[40] has ongoing research activity in digital forensics, critical infrastructure security and cyber education.

Based at ECU, the National Cyber Security Cooperative Research Centre[41] works on building capability and capacity and collaborates with industry and universities to accelerate research and development of practical, evidence-based solutions to critical cybersecurity problems.

The Western Australian Police Force has located its Technology Crime Services headquarters at ECU, which places the university at the forefront of tackling the challenge of cybercrime by providing police investigations with additional expertise.

3. Mission Meetings and Discussions

3.1 Canberra Cyber Hub

The Canberra Cyber Hub works with industry and other local stakeholders to make Canberra the place to start a business and build a career in cybersecurity. Alongside this, they highlight the talent and innovative companies already part of the local ecosystem. The hub is working on developing long-term programmes to support local companies, sandpit events to foster collaboration between researchers and industry and the development of work-integrated learning programmes.

The focus areas are:
- Skills development through education and training.
- Growing and promoting research activities.
- Supporting cybersecurity companies to grow and attract investment.
- Promoting capabilities in the territory.

The main opportunities for cybersecurity companies within Canberra are in the federal government, defence and risk management.

3.2 Ambassador for Cyber Affairs and Critical Technologies (Federal Government – Department of Foreign Affairs and Trade)

Cybersecurity is now viewed as a mainstream issue by the government. The role of the ambassador is to coordinate across government and trade and collate a view on everything into a cohesive whole.

Geopolitics and the COVID-19 pandemic have accelerated digital transformation in recent times, which is having a demonstrable impact. It has shown what is possible, including within the government. The Ukraine crisis has brought more consensus and helped to catalyse the agenda amongst allies.

The International Engagement Strategy covers the following areas:
- Influencing global standards and driving towards common or equivalent frameworks between key partners.
- Ethical issues especially focused on gender and diversity. The aim is to ensure inclusivity and have the mechanisms in place to mitigate against the potential negative impacts of technology and cyber.
- Establish and promote international law and norms and ensure that they are upheld.
- Protecting intellectual property (IP), and safeguarding it in Australia – legislation has recently (in the last five years) been reshaped and adjusted to provide additional protections.
- Market access in an equitable, transparent and reassuring way.
- Protect critical supply chains.

Within Australia the rise in “Digital Natives”, people going online for the first time, has put an increased number of people at risk, and this new group is most vulnerable. As a result, there is a concerted effort to promote basic cybersecurity awareness and knowledge to protect against the most basic risks and scams.

There has been significant investment in capacity building (over A$100 million) to get industry working with the federal government to uplift capability and capacity. The growing investments in digital technologies in the Indo-Pacific present an opportunity as large parts of the region are still to be connected and, as they are, that brings risks which provide opportunities for the cybersecurity companies in the region. Australia seeks to gain influence at all levels across the region to forward their strategic ambitions.

The UK-Australia Technology Partnership[42] is a bilateral effort to build a long-term joint vision for engagement – business to business, but also the wider issues where the two countries have shared interests diplomatically and on strategic technologies.

3.3 Cyber Security Cooperative Research Centre (CRC) [43]

Cooperative Research Centres (CRC) is a federally funded programme.[44] The Cyber Security CRC is focused on growing cybersecurity capability and capacity with a view to making Australia a safer place to live and work. They do this primarily by working on the development of innovative applied research and nurturing the best minds to solve critical cybersecurity challenges. Industry collaborates with universities to obtain federal government funding with research themes across critical infrastructure security and cyber-as-a-service. There are 113 PhD and Masters academics in the programme.

The approach is also designed to accelerate the release of IP from universities into public use and make it accessible to industry. A 2021 report provides some in-depth detail of the programmes that are supported. A diversity of projects is being undertaken.[45]

Some examples of what has been supported include:

- Software security with a focus on Critical Infrastructure – Looking at software Bill of Materials (BOM) issues in the supply chain.
- Critical infrastructure providers and protections. The project looks at human behaviours which have been learnt over time. Machine learning then leverages that and acts as an assistive asset.
- Designed a "game" for non-executive directors to help them understand risk appetite and what's happening in the cyber area.

3.4 Australian Federal Government – Department of Home Affairs[46]

The Department of Home Affairs' role is to lead the development of cybersecurity policy for the Australian government. This includes the overall implementation of the Cyber Security Strategy 2020[47] and the Ransomware Action Plan.[48]

The Australian Cyber Security Strategy is being updated, and there is now a whole-of-the-nation approach rather than just a pure focus on protecting critical national infrastructure. The Optus breach has focused minds across Australia, and cybersecurity and data privacy are getting far more attention. The Optus breach compromised the personal data of approximately nine million people.

The belief within Australia is that the country is well prepared to deal with network security; however, this was an API (Application Programming Interface) vulnerability. Security is still an afterthought for many organisations running applications and services where large volumes of critical data are moved around through APIs. Australia has domestic support to mitigate the impact of such vulnerabilities[49]. However, it still doesn't appear high on the list of priorities. When an individual's identity credentials are compromised in the way that they have been, it isn't something the country has any legal powers over to protect people.

Companies hold vast amounts of data which can lead to trust and assurance issues. A secure identity is a necessity to minimise the impact of another Optus-like breach. Still, there are cultural issues around identity, much like in the UK, and the government doesn't want to be seen as the holder of people's information. There is a belief that some form of "self-sovereign identity" may be the solution; however, this would require a significant set of policy changes, which doesn't appear to be on the horizon in the near future, at least.

The same trust and assurance exist when it comes to the safety of IoT devices. The Australian public has no way of knowing if an IoT device is up to standards or has even the most fundamental protections. On this front, there is no legislation to enforce minimum standards on manufacturers (like the UK Product Security and Telecommunications Infrastructure (PSTI) Bill)[50], and very poor general public education around these sorts of issues.

There is a recognition that there needs to be a much more robust rigorous approach; however, it doesn't appear to be on the horizon. Citizens need confidence in the services they can use, and voluntary codes don't seem to have had much impact to date.

There is a need to find the right policy levers to make a shift in consumer and market behaviour together with bold regulatory ambition to mandate improvements and bring about market shift.

The 5G case makes the weaknesses even more apparent. Guidance has been issued not to use what are termed high-risk vendors. However, the fact that so few vendors can provide what is required makes this somewhat problematic. There is no real domestic capability, and this sort of dependence is not seen as necessarily a good thing. There remains complacency regarding the security of software supply chains, and there is an increased urgency to understand the vulnerabilities in these supply chains and the potential impact on the whole of the nation.

The commercialisation of IP does not happen domestically in any significant way; therefore, the country is left at the behest of the market. Australia places a high priority on the need to develop sovereign capability so that it is not dependent on the external market. Furthermore, they seek to develop partnerships with their allies to shape and influence market(s) – their structure, dynamics and values.

3.5 International Cyber Policy Centre (ICPC), Australian Strategic Policy Institute (ASPI)[51]

The International Cyber Policy Centre (ICPC) has become a voice in some of the global discussions on cybersecurity, emerging and critical technologies, foreign interference and the destabilising impact of disinformation. It works to set the agenda for these discussions and is particularly interested in the impact of these areas on policy. The centre works on capacity building across the Indo-Pacific through workshops, training programmes and large-scale exercises for the public, private and civil society sectors. In addition, they carry out their own research designed to support and lead policy development.

The research focuses on the following:
- Policy.
- Technical analysis.
- Information operations and disinformation.
- Critical and emerging technologies.
- Cyber capacity building.
- Internet safety.
- STEM education for indigenous communities and women.
- Satellite analysis.
- Surveillance.
- China-related issues.

Providing a mechanism by which assurance and trust can be improved in hardware is also of interest to them. Following a standard and providing a rating is not seen as a practical approach, as it can only provide a snapshot of the security of any device at a given point in time. It doesn't ensure ongoing security.

The Infosec Registered Assessors Programme (IRAP)[52] is the regulatory framework which endorses suitably-qualified cybersecurity professionals to provide relevant services which aim to secure broader industry and Australian government systems and data.

Development of sovereign capability is also an area of interest, and they see working with friends and allies through existing established forums and channels like AUKUS as something that should be more actively pursued.

In terms of raising standards overall, they see the approach as one where industry and government need to collaborate to identify the core components of "good cyber" and develop a framework by which organisations can implement and prove adherence.

3.6 Canberra Innovation Network (CBRIN)[53]

Canberra Innovation Network (CBRIN) is a not-for-profit that opened in 2014. It represents a collaboration between local education and research institutes. They support entrepreneurs with ideas to turn them into viable and future high-growth companies. They see themselves as connectors and coordinators of the innovation ecosystem in Canberra. They are sector agnostic but do, and have, supported local cybersecurity companies as part of the cohorts that have come through the programmes they offer. Approximately 10,000 people a year engage with CBRIN. The services they offer include:
- Run events for target audiences such as entrepreneurs, researchers and investors.
- Co-working space.
- Accelerator programme in collaboration with private investors.
- Innovation Connect – prototyping hub and A$30,000 funding (Dragons Den type selection process).
- Incubator – scale-up programme for those that are post-funding or post-revenue.
- Collaborative innovation lab – collective intelligence design consulting service – coming together to solve complex problems.
- Research to impact programme – a programme to leverage academic ideas – help academia to understand the potential.

CBRIN is also supported by corporate sponsors, for example:
- Optus gives free internet access.
- PWC provides management consulting and accountancy services.

An example of a CBRIN success story is Insta-Cluster which was sold to NetApp for A$750 million eight years ago. They grew from two to thirty-five employees and have gone on to have over 300 employees worldwide. NetApp now has a space in Canberra, which has proven to be great for the region bringing more money and fresh eyes.

3.7 Director of the Tech Policy Design Centre at ANU[54]

The Tech Policy Design Centre is part of the Australian National University (ANU) in Canberra. They work on developing policy frameworks and structures that are aligned with the accelerated pace of digital innovation with the aim of creating a more suitable mature tech-governance ecosystem.

The work to date has identified that Australia has problems with regulating technology effectively. This problem is further exacerbated as it isn't clear who the regulator should be either. A report published by the centre compared 13 jurisdictions internationally, including the UK, China and the US, to see how countries are organising themselves in terms of regulatory capacity. The findings showed that only six of those jurisdictions had mandatory powers, and the ability to compel cybersecurity into the private sector. Few have used their powers.[55]

The Australian Cyber Security Centre is not the regulator; they are the respondents. In Australia, the Department of Home Affairs has the authority to regulate.

Findings from the Australian National Audit Offices Review (ANAO)[56] report New Powers and Mandates[57] are damning on the capacity of the Cybersecurity Centre. The findings indicate that:

- No policy/procedures to assess the level of competence and confidence.
- No staff in positions or certain roles.
- Powers are not being enforced even though the Australian powers are some of the most powerful in the world.

It's not enough to give powers to an agency; a structure needs to be in place for those powers to be effective. Otherwise, confusion ensues, and it becomes an administrative overhead.

3.8 Canberra Cyber Ecosystem Research Expertise and Unique Cyber Capabilities

The companies from Canberra that presented were:
Quintessence Labs aims to support organisations to become quantum resilient. This includes solutions for quantum-enabled key generation, crypto-agile key and policy management through to quantum key distribution. https://www.quintessencelabs.com/
Penten provides secure mobility solutions to securely access classified information and support highly complex but simple-to-use, secure communications technology for the tactical environment. https://www.penten.com/about/
Castlepoint Systems provides governance, risk management and compliance solutions. https://www.castlepoint.systems/
ArchTIS provides software solutions for the secure access, collaboration and sharing of sensitive, classified and top-secret information. https://www.archtis.com/
SlicedTech is a managed service provider supporting government and business with the development and deployment of secure, scalable and robust IT solutions. https://slicedtech.com.au/
Cognitive Advantage offers consulting and systems integration services to government and defence industry. Specialises in operational technologies for the defence, national security, and law enforcement sectors. https://cognitiveadvantage.com.au/
Blue Eagle Technologies specialises in designing and supplying high-security IT services, data protection and vulnerability prevention. https://www.blueeagle.technology/company/
OPES Cyber Security works to implement innovative and sovereign solutions to complex problems within the Australian National Intelligence Community. https://opescyber.com.au/about-us/
Blue Phoenix Systems is a cybersecurity consultancy supporting businesses to improve their cybersecurity posture and to become cyber resilient. https://www.bpsystems.com.au/

All the companies primarily target the government and the defence sector as customers. In many cases, this meant that employees needed security clearance which adds to the complexity brought on by the skills shortage as non-citizens are not eligible for security clearance.

The significant benefit of Canberra from the point of view of the customer base is that the maturity of the clients is better than in other parts of the country. Cyber risks are better understood by people in the federal government which is a significant advantage. However, sales cycles can be long, and the procurement process isn't necessarily straightforward.

Start-ups have a difficult time getting a first customer as the government and the defence sector are risk averse, so you need to have a track record to be taken seriously. It is also the case that the network of connections plays a big role in success. If you can get the right people to make introductions, that is also a significant benefit and can accelerate market access.

Partnering with some of the big incumbents is another approach these companies use. This is not unusual and is the case in other parts of the world when a small company targets the government or a large multinational company. Whilst this can be a successful approach, there are better ways to become known, which can mean the company is independent of these partnerships in the long term.

3.9 University of New South Wales (UNSW) Canberra – Launch on Northbourne[58]

Launch on Northbourne is a co-working space designed to promote collaboration and innovation, bringing together academics, businesses, government and the wider ACT community to develop and grow the local defence and security capability and technologies.

The plan is to do this on a much larger scale at UNSW's planned Defence and Security Innovation Precinct at the new UNSW Canberra City campus.

This appears to be unique in that it provides a facility where work requiring government-mandated security is facilitated whilst maintaining the open environment needed for collaboration and knowledge exchange.

3.10 University of New South Wales (UNSW) Canberra[59]

University of New South Wales (UNSW) Canberra has a specific focus on defence and security. At UNSW Canberra Australian Defence Force Academy (ADFA) trainees can get a degree alongside their military training.

The cybersecurity research covers the following areas[60]:
- Resilient infrastructure.
- Situational awareness.
- Cyber war: ethics and policy.
- Complex systems security.
- Human factors in cybersecurity.
- Information influence and war gaming.
- Intelligent security.
- Useable security and value-sensitive design.
- Trusted autonomy.
- Values in defence and security technology.
- Cyber-physical systems.
- Applied and industrial mathematics.
- Behavioural science.
- Cultural geography.
- International ethics.
- Conflict and society.

Additionally, they are working on developing an end-to-end cybersecurity learning framework. This incorporates cyber literacy through to professional certifications.

They also focus more on problem-centric research, which is practitioner initiated/led. There is a strong ambition for tangible research outcomes that result in solutions.

Ongoing Collaboration

The UK National Cyber Security Centre (NCSC) provides financial support to researchers at UNSW to accelerate their work on the development of their seL4 microkernel technology.[61] The technology aims to protect the safety, mission and security-critical systems from cyberattacks. The work is being carried out by the Trustworthy Systems Group at UNSW and is led by Professor Gernot Heiser, the original inventor of the technology.

NCSC is evaluating the seL4 microkernel technology and has ongoing collaborations with the defence industry to get initial real-world deployments. It is a technology that is already in use in civilian applications. The NCSC support aims to test and evaluate the technology in more complex systems and embedded devices.[62]

3.11 Australian National University (ANU)[63]

Australian National University (ANU) offers a number of study programmes in cybersecurity which covers foundation topics through to a Master's programme which includes cybersecurity and risk management. The university has a direct relationship with the defence sector and specifically the Australian Signals Directorate (ASD).[64]

Specific areas of research include:
- The full stack of hardware and software.
- Formal methods/theorem proving/formal verification.
- Software testing and verification at scale.
- Formal verification of network protocols.
- Cyber threats to the electronic voting system.
- Zero-knowledge proofs.
- Data privacy.

3.12 Canberra Institute of Technology – Department of Cyber Security[65]

The Department of Cyber Security at the Canberra Institute of Technology is developing courses providing micro-credentials in specific competencies and capabilities alongside other vocational courses in cybersecurity. The courses are available as apprenticeships, traineeships or Australian School-based Apprenticeships (ASbAs).

The aim is to support up-skilling and re-skilling through these courses. ACT government employees would not be able to get any funding to take these sort of courses – they can do them but would need to find other sources of financial support.

There is no cybersecurity degree apprenticeship programme; however, the Australian government runs a digital cadetship programme. The programme aims to bring young digital talent into government. To be eligible, you must be an Australian citizen studying for an undergraduate or postgraduate degree in a digital or technology-related field. The programme provides a placement/internship within the government and its agencies. The aim is to provide them with practical skills through a wide range of digital roles.[66]

3.13 Oceania Cybersecurity Centre (OCSC)[67]

The Oceania Cybersecurity Centre (OCSC) is working to strengthen cybersecurity (capacity and maturity) in the Indo-Pacific region. It has a twofold approach to this:

- Conduct cybersecurity assessments in countries, at the invitation of a government, to help to understand the respective country's cyber maturity, identify next steps to improve, and provide evidence-based recommendations that will contribute to the country's policy frameworks, strategies and activities towards becoming more resilient and enhancing the overall cyber capacity.
- Advance cybersecurity education and research to build digital resilience in Australia and the Indo-Pacific as a whole.

The assessment work is based on the University of Oxford Cybersecurity Capacity Maturity Model for Nations (CMM).[68] From the assessment, a country's cyber maturity can be defined as being at any one of five different stages. The stages define the level of progress the country has made in relation to a certain factor or aspect of cybersecurity capacity. The model derives from the Capability Maturity Model developed by the Software Engineering Institute at Carnegie Mellon University in Pennsylvania, USA. The original model assessed the level of maturity of an organisation's software engineering capability, where Stage 1 meant there was no evidence of any defined processes through to Stage 5, where there was a fully operational optimised repeatable process which meant the highest qualities could be continually maintained.[69]

Eight Pacific islands have been assessed so far. The hope is that this approach will help bring alignment amongst the Indo-Pacific nations around recognised best practices and standards and enforce regional transparency and trust. Solutions to problems discovered in the poorer economies must then be delivered through aid budgets and/or multilateral organisations. An alternative for financial support is capacity-building funds that the private sector invests in from time to time.

Research and education activities that are underway include:

- Thought leadership.
- University internships.
- Research grants.
- Education seminars.

The work of OCSC is supported in monetary terms by the United Kingdom Foreign and Commonwealth Development Office (FCDO) and the Victoria State government.

3.14 CyRise[70]

CyRise is a cybersecurity accelerator launched in 2017. It is based in Melbourne and is expanding to Sydney this year. It is hosted by Stone and Chalk.[71] It is the only dedicated cybersecurity accelerator in the Asia Pacific region. The closest next one is in Singapore – ICE-71.[72]

CyRise sees itself as an investor, supporter and champion of cybersecurity start-ups in the Asia Pacific. It runs a 14-week programme and provides the start-ups with initial funding of A$50K in the form of a safe note (taking 4-5% equity). They have, to date, run six cohorts, and the geographic representation has included companies from Australia, New Zealand, Singapore and the US. UK companies are welcome to join; however, virtual participation is hampered by the time difference between the two countries. The alternative would be that the companies would have to spend at least 14 weeks in Melbourne. The next intake will be in February 2023.

Mentors play an active role in supporting the companies; they must have a genuine interest and be willing to give up to six hours of their time. There is a network of over 60 Chief Information Security Officers (CISOs), and they are looking to broaden their partnerships.

Companies that have been through CyRise have raised more than $37.5 million (spread across 34 investments). The value of the full portfolio of companies from the six cohorts is approximately $193 million, creating 97 jobs.

CyRise also runs bootcamps for people who just have an idea, and an Elevate programme designed to support the growth of ambitious people already in the sector.

CyRise plans to launch a scale-up programme in July 2023 based at the new Stone and Chalk facility in Sydney in the heart of the new Tech Central area. This programme will primarily be pitched at pre-series A and B companies.

Finally, there is an aspiration to build a fund to support pre-seed and seed-stage investments for cybersecurity start-ups.

3.15 Grok Academy[73]

Grok Academy is a not-for-profit with a mission to educate young children in core computing skills, including cybersecurity. They have a Learning Platform[74], which has a library of online courses, activities and competitions aligned with the Australian National Curriculum with respect to the learning requirements for digital technologies.

Over 210,000 children have participated in cybersecurity challenges provided through the learning platform. The challenges are developed in collaboration with personnel from the Australian cybersecurity sector. They are designed to allow students to gain experience as a real-world hacker or cybersecurity specialist. Industry sponsorship, including from BT in the UK, has allowed them to provide access to these challenges for free to children in school years 3 through to 12 across Australia.

They are looking to expand their coverage and have a definite interest in trying to find mechanisms by which this can be brought to the UK.

3.16 Australia's Academic and Research Network (AARNET)[75]

Australia's Academic and Research Network (AARNET) provides services and support for the research and education community across Australia. This includes telecoms services, alongside a range of cybersecurity, data and collaboration services, designed to meet the very specific needs of the community they are servicing. The community includes Australian universities and the CSIRO, as well as many health and other research institutions, cultural organisations, schools, vocational training colleges and specialist content providers.

Australian universities have signed up to the Defence Industry Security Program.[76] AARNET supports this by providing the required infrastructure for secure collaborations in order to carry out classified research.

3.17 Enex TestLab[77]

Enex TestLab provides the capability to test and evaluate products, services and systems. They specialise in a broad range of services which include:

- Product testing.
- Certification and verification.
- Type approval testing.
- Benchmarking.

Testing is typically carried out against a standard; however, on occasions testing and benchmarking are against criteria set down by the customers either because there is no available standard and/or because they are contractually committed to supplying the product or service that meets those minimum criteria.

Testing is not mandated in Australia in most areas, so most businesses do not do it, as the time and cost overheads make this an unattractive voluntary undertaking. Regulation tends to follow the UK but generally lags by a few years, so testing in some areas is likely to become mandatory in the future.

3.18 MITRE[78]

MITRE is a US company focused on providing services to support the national security agenda within the US. They have recently set up an office in Adelaide, Southern Australia, primarily to exploit the opportunities that may arise in the same context, especially from the increased bilateral activity between Australia and the US.

3.19 Tech Central[79]

Tech Central aims to create a "branded community"' in the heart of Sydney that brings together three universities, a research hospital and over 100 research institutes and centres of excellence alongside existing hubs and communities of start-ups in the six neighbourhoods that Tech Central will span. The ambition is to drive growth and impact by bringing a critical mass of the brightest minds together in close proximity, so as to bring about more disruptive innovation, collaboration, exchange of ideas, and to explore new markets.

The NSW government has launched an A$8 million Tech Central Research and Innovation Infrastructure Fund. The fund aims to support and accelerate the development of physical and digital infrastructure within Tech Central alongside the expansion of technical expertise, collaboration and commercialisation in target industries and areas of research.[80]

3.20 The Commonwealth Scientific and Industrial Research Organisation (CSIRO)[81]

The Commonwealth Scientific and Industrial Research Organisation (CSIRO) is a government agency responsible for scientific research. CSIRO works with leading organisations around the world. They are Australia's national science agency and innovation catalyst and have 5,500+ people over more than 50 sites with 300+ PhDs. They have more than 200 government and corporate sponsors.

They undertake what is termed mission-driven science and are, from that perspective, one of the world's largest mission-driven multidisciplinary science and research organisations. They look to leverage their research and collaborations worldwide into the policy-making activities of other parts of government. The main focus of the research is around six challenges:

- **Food security and quality:** achieve sustainable regional food security and grow Australia's share of premium agrifood markets.
- **Health and wellbeing:** help enhance health for all through preventative, personalised, biomedical and digital health services.
- **Resilient and valuable environments:** enhancing the resilience, sustainable use and value of Australia's environments, including by mitigating and adapting the impacts of climate and global change.
- **Sustainable energy and resources:** build regional energy and resource security and competitiveness while lowering emissions.
- **Future industries:** help create Australia's future industries and jobs by collaborating to boost innovation performance and STEM skills.
- **A secure Australia and region:** help safeguard Australia from risks (war, terrorism, regional instability, pandemics, biosecurity, disasters and cyberattacks).

3.21 CSIRO Data61[82]

Data61 is the data and digital specialist arm of CSIRO. Their research expertise includes AI, robotics, cybersecurity, modelling and analytics. They have generated over 18 spin-outs and hold over 130 patents. Approximately 70% of the research is theoretical, whilst the rest is in collaboration with industry with an applied focus.

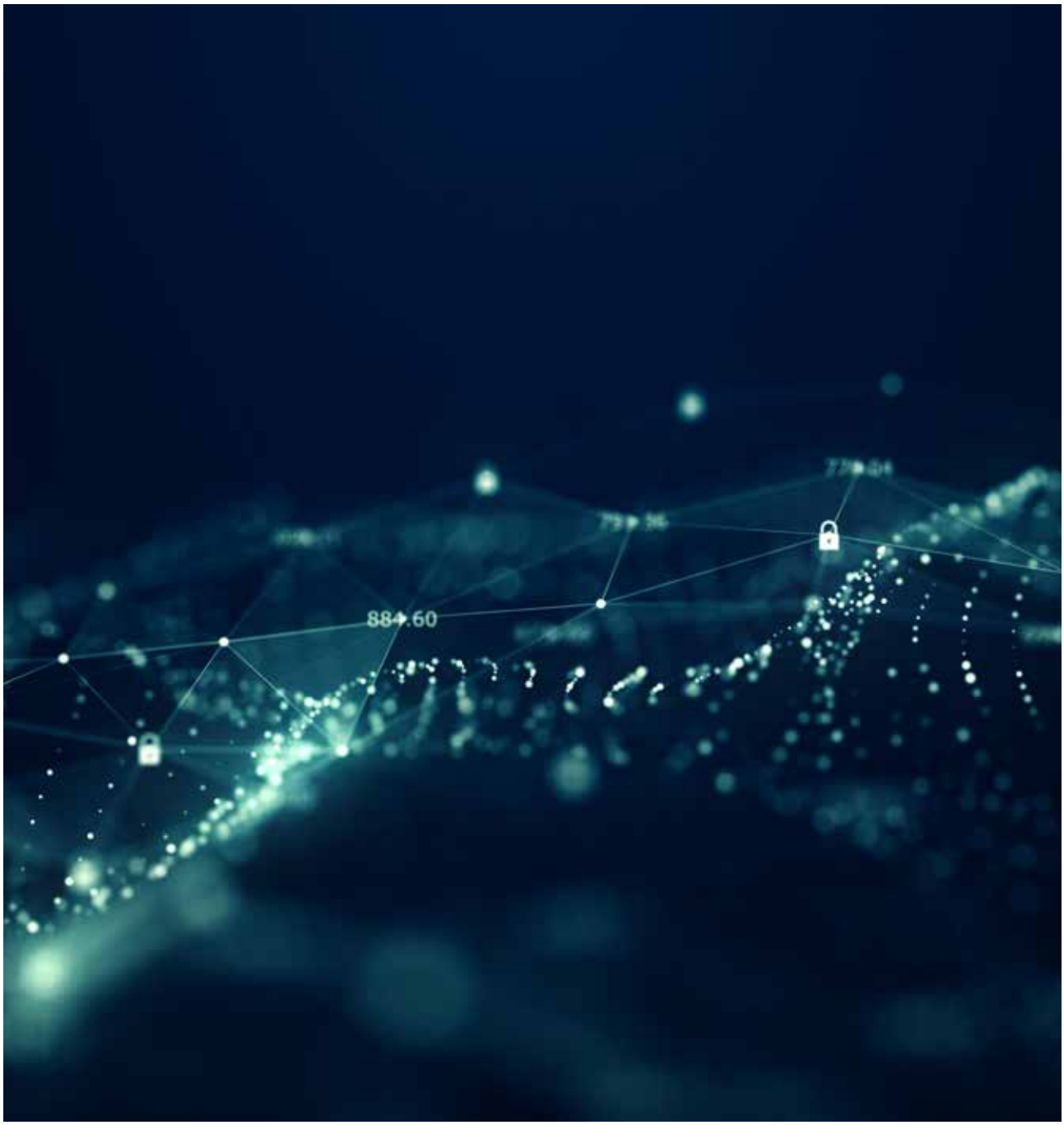
In the cybersecurity area, they have more than 40 members of staff and 50 PhDs. They have received A$8 million in funding from the defence sector to advance some of their research.

Their work in cybersecurity is focused on the intersection of quantum, the human and AI to see if we can use the critical emerging capability to drive solutions for cybersecurity. They have a specific interest in quantum safe algorithms and quantum key generation, although there appears to be little evidence of new work. The more blue-sky work looks at topics like how humans and machine learning can work together. Other than that, they have a similar focus on some of the known global challenges but appear to have very little sight of other work, which as a result, seems to be limiting innovation or knowledge creation.

They are very keen to get the technology they develop used in the real world. To enable this, they partner with business, and on some occasions a spin-out results.

They have ongoing collaborations with the University of Cardiff and the University of Newcastle, supported by EPSRC-funded projects and with the Alan Turing Institute.

Other international collaborations include:
- Joint funding programme with the US National Science Foundation on Responsible AI.
- Partnership with Boeing on IoT security.
- Ongoing negotiation with CIFAR in Canada.



3.22 University of Technology Sydney (UTS)[83]

University of Technology Sydney (UTS) is ranked the best nationally in both telecommunication engineering and computer science. Globally it ranks sixteenth and eleventh, respectively.

The university is building the UTS Vault, a secure collaborative research and innovation facility. It is part of a A$250 million investment from the NSW government to accelerate growth in the industries of the future. The vault should enable collaboration between private sector users and a university to advance research and commercialisation in cybersecurity and defence technology. It will provide a place where the private sector can experiment with new technologies and ideas whilst de-risking those experiments from some of the otherwise critical operational risks that would potentially prohibit such innovation and research activities.[84] As such, it should unlock innovation and create pathways for commercialisation bringing government, industry and academia together. Within the vault, the Zone 3 & 4 facility will be based on the Australian Information Security Manual and Protective Security Policy Framework.

UTS has a Centre for Quantum Software and Information working on developing software and the infrastructure for future quantum technologies.[85]

Additionally, they are building a Security Operations Centre (SOC)/War Room to develop the next generation of cybersecurity professionals.

3.23 Stone and Chalk[86]

Stone and Chalk are primarily a co-working space provider. Within that co-working space, they host start-ups and scale-ups covering a broad range of technology areas such as cybersecurity, quantum, artificial intelligence, fintech and IoT, amongst many others. They have three primary facilities across Sydney and Melbourne. In Melbourne, they host CyRise, and in Sydney, they host the Sydney Start-up Hub, and in their new facility, within Tech Central, they plan to host scale-ups, including a new Sydney-based CyRise scale-up cohort. Stone and Chalk's new facility and the scale-up programmes are subsidised by funding from the NSW government.

3.24 AustCyber[87]

AustCyber is the Australia Cyber Security Growth Network. This involves three key activities:

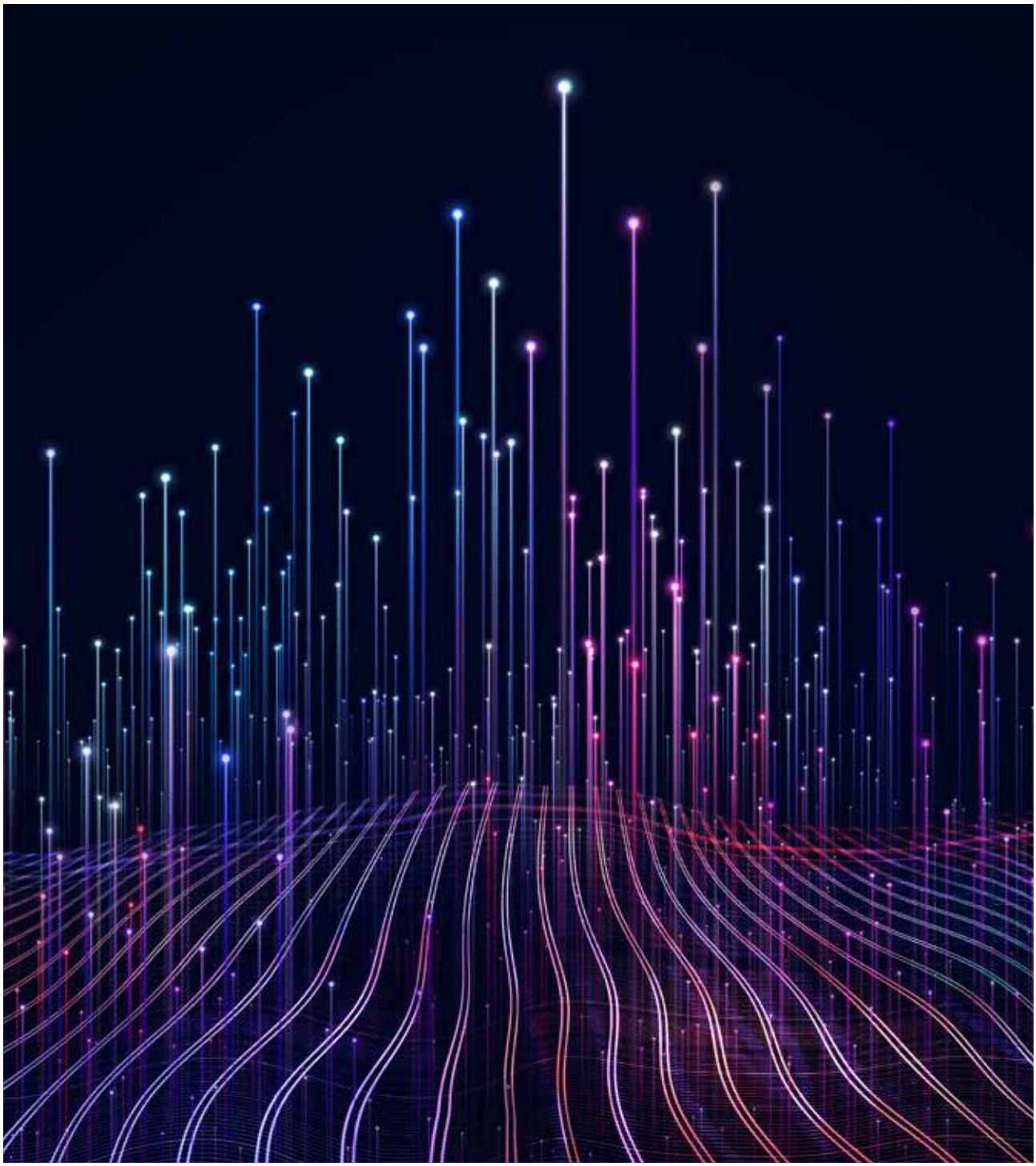
- Growing the cybersecurity ecosystem within Australia.
- Generate export opportunities for the Australian cybersecurity ecosystem.
- Create a world-leading centre for cyber education.

They have established a national network of innovation nodes tasked with accelerating innovation and collaboration in cybersecurity across the country . Each innovation node is focused around the cybersecurity needs and demands of the dominant local industry sectors.

AustCyber was founded in 2017 as an independent not-for-profit entity funded by the federal government.

3.25 Australian Information Security Association (AISA)[89]

The Australian Information Security Association (AISA) is a not-for-profit charity created to bring information security professionals together. The individual membership is now over 9,000, along with a number of corporate sponsors from across Australia. They aim to promote an independent view on key topics and to raise widespread awareness across the country around the threats and risks of cyberattacks and data theft. To achieve this, they have, and continue to undertake, a broad range of initiatives.



Annex 1 –
List of Participants from the UK

Assentian Partners
British Telecommunications (BT)
Darktrace
Department for Digital, Culture, Media & Sport (DCMS)
University College London (UCL)
Utterberry Ltd
Innovate UK

Annex 2 –
List of Participants from Australia

Canberra

ACT Government
Apporetum
archTIS Ltd
Australian Cyber Security Centre (ACSC)
Australian Department of Home Affairs
Australian Federal Government
Australian National University (ANU)
Australian Strategic Policy Institute (ASPI)
Blue Eagle Technologies
Blue Phoenix Systems
Canberra Cyber Hub
Canberra Innovation Network (CBRIN)
Canberra Institute of Technology
Castlepoint Systems
CBR Cyber
Cognitive Advantage
Cyber Security Cooperative Research Centre (CSCRC)
Fifth Domain
Penten
Procurement ACT, ACT Government
QuintessenceLabs
Sliced Tech
Teron Labs
Treasury and Economic Development Directorate, ACT Government
University of Canberra
University of New South Wales (UNSW)
Viden

Melbourne

Australian Cyber Collaboration Centre
Australia's Academic and Research Network (AARNet Pty Ltd)
British Consulate Victoria
Cydarm Technologies
CyRise
Department for Industry, Innovation and Science, Government of South Australia
Enex Testlabs
Invest Victoria
Oceania Cyber Security Centre
Office of the Chief Information Officer, Government of South Australia
Royal Melbourne Institute of Technology (RMIT University)
South Australia Cyber Security Innovation Node AustCyber

Sydney

AustCyber
Australia Information Security Association (AISA)
British Telecommunications
Data 61, CSIRO
Defence Innovation Network (DIN) Australia
Investment NSW
Stone & Chalk
Tech Central
University of Technology, Sydney

References

1. https://www.gov.uk/government/collections/uk-australia-free-trade-agreement
2. https://www.dfat.gov.au/trade/trade-and-investment-data-information-and-publications/foreign-investment-statistics/statistics-on-who-invests-in-australia
3. https://www.gov.uk/government/news/record-levels-of-investment-for-uks-101-billion-cyber-security-sector
4. https://www.gov.uk/government/publications/national-cyber-strategy-2022/national-cyber-security-strategy-2022
5. https://www.gov.uk/government/news/foreign-secretary-statement-cyber-and-critical-technology-partnership-with-australia
6. https://www.trade.gov/country-commercial-guides/australia-cybersecurity
7. https://www.austcyber.com/
8. https://www.austcyber.com/resources/sector-competitiveness-plan/appendix-a
9. https://www.business.nsw.gov.au/innovation-and-research/programs/knowledge-hubs/NSW-cyber-security
10. https://aisa.org.au/Public/NSW-Cyber-Hub/NSW-IPP.aspx
11. https://www.investment.nsw.gov.au/living-working-and-business/sector-opportunities/technology/cyber-security/nsw-cyber-accelerator/
12. https://www.business.nsw.gov.au/innovation-and-research/programs/knowledge-hubs/NSW-cyber-security/nsw-cyber-ambassador-program
13. https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-strategy/our-strategy-glance
14. https://ifcyber.unsw.edu.au/
15. https://www.uts.edu.au/study/find-a-course/bachelor-cybersecurity
16. https://www.mq.edu.au/
17. https://www.investment.nsw.gov.au/
18. https://www.digital.nsw.gov.au/policy/cyber-security/cyber-security-strategy/our-strategy-glance
19. https://www.investment.nsw.gov.au/resources/media-releases/future-economy-fund-to-drive-businesses-and-industries-of-tomorrow/
20. https://www.nsw.gov.au/regional-growth-fund
21. https://www.cyrise.co/
22. https://www.globalaustralia.gov.au/industries/cyber-security/state-ecosystem/victoria
23. https://www.invest.vic.gov.au/
24. https://app.remplan.com.au/eda-victoria/economy/industries/output
25. https://www.bulletpoint.com.au/breakthrough-victoria-fund/
26. https://breakthroughvictoria.com/who-we-are/
27. https://www.canberracyberhub.com.au/

28. https://www.austcyber.com/resources/sector-competitiveness-plan/appendix-a
29. https://www.asd.gov.au/
30. https://www.cyber.gov.au/
31. https://sasic.sa.gov.au/
32. https://lotfourteen.com.au/
33. https://www.austcyber.com/resources/sector-competitiveness-plan/appendix-a
34. https://www.cybercollaboration.org.au/
35. https://www.flinders.edu.au/jeff-bleich-centre
36. https://www.ecu.edu.au/
37. https://www.ecu.edu.au/schools/science/research/strategic-centres/ecu-security-research-institute/about
38. https://www.wacyberhub.org/
39. https://www.industry.gov.au/science-technology-and-innovation/industry-innovation/industry-growth-centres
40. https://www.ecu.edu.au/schools/science/research/ecu-security-research-institute/overview
41. https://cybersecuritycrc.org.au/
42. https://www.gov.uk/government/news/foreign-secretary-statement-cyber-and-critical-technology-partnership-with-australia
43. https://cybersecuritycrc.org.au/
44. https://cooperativeresearch.org.au/cooperative-research/crc-program-australian-government/
45. https://cybersecuritycrc.org.au/case-studies
46. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security
47. https://www.homeaffairs.gov.au/cyber-security-subsite/files/cyber-security-strategy-2020.pdf
48. https://www.homeaffairs.gov.au/cyber-security-subsite/files/ransomware-action-plan.pdf
49. https://www.aiculus.co/
50. https://evalian.co.uk/the-upcoming-uk-iot-security-law-what-you-need-to-know/
51. https://www.aspi.org.au/program/international-cyber-policy-centre
52. https://www.cyber.gov.au/acsc/view-all-content/programs/irap
53. https://cbrin.com.au/
54. https://www.anu.edu.au/research/research-initiatives/tech-policy-design-centre
55. https://www.anu.edu.au/files/guidance/TPDC_Report_NO1_2022_digital_release.pdf
56. https://www.anao.gov.au/
57. https://www.protectivesecurity.gov.au/publications-library/policy-10-safeguarding-data-cyber-threats
58. https://launch.unsw.edu.au/
59. https://www.unsw.adfa.edu.au/about-us
60. https://www.unsw.adfa.edu.au/our-research
61. https://www.ncsc.gov.uk/news/ncsc-joins-the-sel4-foundation

62. https://newsroom.unsw.edu.au/news/science-tech/uk-backs-acceleration-unsw-cyber-security-research
63. https://www.anu.edu.au/
64. https://www.asd.gov.au/
65. https://cit.edu.au/courses/professional/cyber
66. https://www.digitalprofession.gov.au/career-development/emerging-talent-programs/digital-cadetship-program
67. https://ocsc.com.au/
68. https://gcscc.ox.ac.uk/the-cmm
69. https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=11955
70. https://www.cyrise.co/
71. https://www.stoneandchalk.com.au/
72. https://ice71.sg/
73. https://groklearning.com/
74. https://groklearning.com/teachers/australia/
75. https://www.aarnet.edu.au/
76. https://www.defence.gov.au/security/industry
77. https://testlab.com.au/
78. https://www.mitre.org/who-we-are
79. https://www.tc.sydney/
80. https://www.nsw.gov.au/enterprise-investment-trade/media-releases/8-million-tech-central-research-infrastructure-fund-opens
81. https://www.csiro.au/en/
82. https://data61.csiro.au/
83. https://www.uts.edu.au/
84. https://www.uts.edu.au/news/tech-design/uts-opens-vault
85. https://www.uts.edu.au/research/centre-quantum-software-and-information
86. https://www.stoneandchalk.com.au/
87. https://www.austcyber.com/
88. https://www.austcyber.com/grow/collaborate/nodes
89. https://www.aisa.org.au/public/default.aspx

Connecting for
Positive Change.

Innovate UK
KTN

Head Office

Innovate UK KTN
Suite 218 Business Design Centre
52 Upper Street
Islington
London N1 0QH

Telephone: 03333 403251
Email: enquiries@ktn-uk.org
ktn-uk.org
@KTNUK

Contact Persons
Roger Iles
Knowledge Transfer Manager - Global Alliance
roger.iles@iuk.ktn-uk.org