

Canberra Cyber Security cluster

Report for ACT Government

16/12/2020

Prepared by
nous

SECTION 1: EXECUTIVE SUMMARY AND KEY FINDINGS

EXECUTIVE SUMMARY

Harnessing Canberra's unique capabilities in Cyber Security to deliver economic growth

The ACT Government has been facilitating the exploration of a potential Cyber Security Cluster in Canberra. Co-owned, co-led and co-designed by its stakeholders, the Cluster would harness Canberra's unique capabilities to grow ACT's share of this global market; creating jobs and driving economic growth.

Done well, the Cyber Security Cluster will deliver jobs and employment, retain talent, cultivate innovation and generate an export industry, ultimately contributing to the diversification and strengthening of the ACT economy. This will enable Canberra to capture much of the estimated 7,000 new cyber security jobs forecasted and over \$4.6 billion of Australian government investments in research and capability development. It will also contribute to the national strategy by establishing expertise and talent development, benefiting all of Australia.

Research undertaken by the Nous Group (Nous) suggests that Canberra is uniquely well placed to take a lead role in Australia's Cyber Security landscape due to the concentration of key Cyber Security stakeholders (including Federal Government Agencies), world-class education and research capability, the most highly educated workforce in Australia - including the highest levels of specialists with security clearance - alongside a highly networked business and Small and Medium Enterprise (SME) community.

The proposed Cluster would exist both virtually, as a digital portal, and physically as a 'Cyber Security Corridor' that builds on the natural footprint and 'clustering' of cyber security organisations located in Canberra. Based on an assessment of the market opportunity and stakeholder support, the Cluster will address four key themes:

CLUSTER AREAS OF FOCUS

Through our consultation, it was determined that the Cluster should focus on the following areas:

EDUCATION PATHWAYS

ACCELERATING SMEs

RESEARCH

PROMOTION AND BRANDING

The following slides outline the high-level design, approach, and rationale for the proposed cluster model based on our consultations with stakeholders and market analysis.

Through consultation with thirty six stakeholders, **Nous found strong support for a Canberra Cyber Security Cluster**, with stakeholders articulating clear opportunities for the Cluster to address. They also provided key conditions for the Cluster to be successful:

1. Addressing clear market opportunities without duplicating existing activity or networks.
2. Has clear and relevant objectives, is independent and open, and leverages existing assets in Canberra.
3. Starts small, builds engagement and trust with stakeholders over time, and is supported by initial seed funding.

Consultation responses also determined that there should be a staged approach to implementation, developing the Cluster over time (see Section 4 of this report).

NEXT STEPS

- 1 Finalise the Cluster's mission, objectives and strategy with stakeholders.
- 2 Confirm the Cluster's governance and reporting structures.
- 3 Design and build the Cluster's stage 1 operating model.
- 4 Project-manage and risk-assess the Cluster development activities.
- 5 Budget and identify initial source for Cluster funding.

OBJECTIVE AND RATIONALE

Exploring the potential to develop a Cyber Security Cluster

The Cluster is envisioned to position the ACT for job creation and economic growth, facilitate diversification and strengthen the ACT economy; creating a vibrant community that will attract and retain people in the city.

WHY CYBER SECURITY?

The global cyber security market is growing rapidly. Cyber security spending is projected to increase by 86% to US\$260 billion by 2020, with 25% of this expenditure expected to come from Indo-Pacific countries. In Australia, cyber security revenue could grow by 40% to A\$5 billion in the next 4 years, with financial services and Federal Government being the biggest domestic buyers.

WHY CANBERRA?

Canberra is well positioned to be Australia's leading city for cyber security due to its:

- high concentration of cyber security stakeholders
- established education and research capabilities
- highly skilled and suitably security cleared workforce
- highly networked business community
- close geographical proximity to key cyber stakeholders.

WHY A CLUSTER?

A Cluster is the ideal platform for this cyber security initiative because it allows key parties to:

- address drivers of growth and opportunities that require collaborative effort
- compete with collaborative models emerging locally and overseas
- simplify an otherwise complex cyber landscape
- grow the ACT's collective share of the cyber security market.

Building on initial discussions about the Cluster with key stakeholders, ACT Government sought to facilitate engagement around three key questions shown below. This report provides the rationale and appropriate concept model for such a Cluster in Canberra.

THREE KEY QUESTIONS GUIDED THE EXPLORATION AND DEVELOPMENT OF THE CLUSTER

Is there sufficient support from key stakeholders for the development of such a cluster?

What will the model for the Cluster look like?

What are the immediate next steps to successfully develop the Cluster?

WHAT WILL THE CLUSTER LOOK LIKE: KEY THEMES

The Cyber Security Cluster will create jobs and drive economic growth by addressing untapped opportunities and fostering collaboration to grow ACT's share of the cyber security market in four key areas

This objective, mission and the four key themes were identified by key stakeholders in the Canberra Cyber Security ecosystem. Section 2 explores each of the four themes in greater detail.

The Cluster's objective	Job creation and economic growth in the ACT through a Cyber Security Cluster
The Cluster's mission	Grow ACT's share of the national and international cyber security market for education, SMEs, research and jobs
It will do this by addressing four key themes	 1. Education pathways: growing Canberra's share of the national and international market for cyber security education.
	 2. Accelerating SMEs: supporting the growth of SMEs by facilitating connections with buyers and investors as well as removing key barriers.
	 3. Research: showcasing the ACT's research successes and capabilities.
	 4. Promotion and branding: promoting and showcasing Canberra's education, research and SME capability through the establishment of a distinct brand and identity.
It will be underpinned by	A governance structure that represents and promotes shared -ownership of key stakeholders

TABLE OF CONTENTS

ITEM	PAGE
SECTION 1: EXECUTIVE SUMMARY AND KEY FINDINGS	
EXECUTIVE SUMMARY	3
OBJECTIVE AND RATIONALE	4
WHAT WILL THE CLUSTER LOOK LIKE: KEY THEMES	5
SECTION 2: EXPLORING THE KEY THEMES	
DETAIL OF THE KEY THEMES	8-11
GOVERNANCE APPROACH	12
SECTION 3: CASE FOR THE CLUSTER	
WHY CANBERRA?	14
WHY A CLUSTER?	15
WHAT IS THE MARKET OPPORTUNITY FOR CYBER SECURITY?	16-21
SECTION 4: A STAGED IMPLEMENTATION APPROACH	
AN OVERVIEW TO THE IMPLEMENTATION APPROACH	23
DETAIL OF CLUSTER DESIGN FOR STAGES 1,2 AND 3	24-29
WHAT ARE THE NEXT STEPS TO IMPLEMENT THE CLUSTER?	30
SECTION 5: APPROACH AND METHOD	
OUR APPROACH	32
WHAT DID WE HEAR FROM STAKEHOLDERS?	33
HOW DID WE PRIORITISE CLUSTER FUNCTIONS AND ACTIVITIES?	34
APPENDICES	36-47

SECTION 2: EXPLORING THE KEY THEMES

THEME 1: EDUCATION PATHWAYS

1

RATIONALE / MARKET OPPORTUNITY

- There is a significant underlying market opportunity with growth in demand for cyber security skills. Growing ACT's share of this global education market will create new jobs and drive growth.
- There is a cyber talent shortage in Canberra, with demand by government, primes and SMEs outstripping supply of job-ready talent. Filling these gaps will drive productivity and growth.
- There are significant opportunities in the current Canberra education landscape e.g., accredited and non-accredited short courses.
- Demand for cyber skills is changing, with employers seeking general and cross-disciplinary capability alongside technical cyber expertise, which Canberra is well-suited to deliver.
- There is specific Federal Government funding available to tap into to support job-ready training e.g. JobTrainer.

2

SUPPORT FROM STAKEHOLDERS

- There was strong support for helping prospective students navigate the complex pathways and options into the industry, with some support for exploring the development of new pathways that address both the need for the general and specialist cyber security skills.
- There was strong support for the development and promotion of clear education pathways for cyber, including non-technical related areas and employer-focussed short-courses or micro-credentials to develop job-ready talent.
- There was strong support for increasing exposure of Canberra's education pathways to prospective students from Australia and internationally in the first instance, progressing to exploring potential for recognition of courses and units to increase attractiveness to prospective students.

3

CLUSTER ACTIVITIES (STEADY STATE)

- Provide a virtual education portal to enable prospective students to learn about and navigate the education pathways in Canberra with ease.
- Conduct regular analysis of industry, workforce and student needs; facilitate development of new education and training offerings across the training needs spectrum (from specialist cyber security training to cross-disciplinary cyber offers) amongst education providers in the ACT; and explore the potential to extend Canberra's educational pathways into growing areas such as micro-credentials and short courses.
- Support recognition of programs and units of study (both accredited and non-accredited) between different education providers in the ACT.

4

CLUSTER ACTIVITIES (YEAR 1)

- Develop and launch the virtual education portal on the Cluster website.
- Promote existing education pathways to prospective students and employers, providing clear information, advice and guidance (IAG), including non-accredited short courses available from private providers.
- Conduct initial analysis of industry, workforce and student needs and initiate discussion about the development of new education and training offerings that will meet employer needs.
- Facilitate identification and development of work integrated learning, student placement, internship, apprenticeship and graduate pathway opportunities for ACT education providers with industry and research partners to include in portal.

THEME 2: ACCELERATING SMEs

1

RATIONALE / MARKET OPPORTUNITY

- There is potential for ACT cyber security businesses, including SMEs, to better attract the growing pool of foreign direct investment and venture capital, creating new jobs and driving growth.
- Cyber security venture capital investment has nearly doubled over the past 15 years from \$US4.7 billion in 2006 to \$US9.9 billion globally in 2019.
- However, Australia significantly lags behind comparable economies in attracting cyber security investment for its start-ups. For example, Israel has approximately 25 times more VC cyber security funding per capita compared to Australia.

2

SUPPORT FROM STAKEHOLDERS

- There was strong support for removing barriers to entry for SMEs. The most significant being to obtain the first customer/client, particularly where government is the main prospective buyer of the product or service.
- There was strong support for the Cluster to establish a network of key cyber security players nationally and internationally, and to facilitate connection and collaboration between organisations.
- There was strong support for the Cluster to advocate for reforms in government procurement. The purpose being to remove barriers to successfully engaging government clients at the state and Federal level, including governments' lack of appetite, resources and tools to work with cyber SMEs. Stakeholders suggested advocating for a model like the Defence Innovation Hub.

3

CLUSTER ACTIVITIES (STEADY STATE)

- Promote the capabilities and improve the collective exposure of SMEs in Canberra, celebrating the success of collaborative innovations between SMEs, industry and government.
- Facilitate connections between sellers, buyers and investors of cyber security products and services through initiatives that increase discovery and matching of stakeholders, such as networking events, a digital marketplace or match-making program.
- Advocate for and facilitate improvements in government procurement processes to address barriers faced by SMEs face in engaging with government clients.

4

CLUSTER ACTIVITIES (YEAR 1)

- Launch networking events in collaboration with partner organisations to connect SMEs with other cyber stakeholders.
- Develop and maintain a network and database of national and international cyber stakeholders including potential buyers and investors.
- Launch a virtual directory of cyber SMEs and stakeholders, which may be developed further into a marketplace that connects prospective sellers, buyers and investors of cyber security products and services.
- Conduct initial analysis of industry cybersecurity innovation needs, government procurement priorities and approaches and provide recommendations to address barriers to entry.
- Advocate for changes to government procurement at the state and Federal level to enhance the success of SMEs engaging government.

THEME 3: RESEARCH

1

RATIONALE / MARKET OPPORTUNITY

- Canberra is home to established education research institutions in ANU, UNSW Canberra, University of Canberra and; the National Computational Infrastructure (NCI); Data61 and CSIRO. These institutions collectively provide a concentration of world-leading cyber security research capability that is unmatched by other Australian cities.
- Global investment in Cyber Security research is growing rapidly. In Australia, there are multiple Federal Government research funding initiatives totaling \$2.9 billion (on top of the \$1.67 billion Cyber Security Strategy 2020 funding commitment) that explicitly supports cyber security research or lists cyber security research as a priority research area.

2

SUPPORT FROM STAKEHOLDERS

- There was strong support for the Cluster to showcase and promote both the success and Canberra's capability for research, in order to compliment existing efforts by individual institutions and organisations such as CRC to attract and facilitate increased research investment.
- Stakeholders agreed that immediate opportunities to facilitate new research collaborations are limited in this space as it is complex environment to navigate.
- However, alongside promotion and profile-raising activity, there was support for the Cluster to facilitate business relationships between research institutes and prospective Australian and foreign research funders.

3

CLUSTER ACTIVITIES (STEADY STATE)

- Analyse and share information on collaborative research opportunities with research providers.
- Facilitate business relationships between research institutes and prospective Australian and foreign research funders.
- Explore options for increased Canberra-based research collaboration across and beyond the cluster in order to attract large-scale funding opportunities.
- Develop a shared understanding of how the different research providers might leverage their individual strengths and niches to contribute to collaborative research.

4

CLUSTER ACTIVITIES (YEAR 1)

- Showcase research successes to date through articles on the website and media press releases.
- Publish a directory of research institutes and experts to facilitate discovery of Canberra's research capabilities
- Analyse and share information on collaborative research opportunities with research providers.

THEME 4: PROMOTION AND BRANDING

1

RATIONALE / MARKET OPPORTUNITY

- Canberra is already a natural hub for cyber security. It has:
 - Australia's highest concentration of Federal Government agencies, prime contractors, and small-medium enterprises engaged in cyber security.
 - Established education and research capabilities in ANU, UNSW Canberra and University of Canberra.
 - A highly skilled and suitably security cleared workforce.
 - A highly networked business community and strong relationships between key stakeholder groups.
 - Geographical proximity to key cyber stakeholders, researchers, businesses and government departments.
- A clear and distinctive identity and value proposition, alongside a coordinated effort to promote Canberra's cyber security capabilities, could increase ACT's share of the global market; creating new jobs and driving economic growth.

2

SUPPORT FROM STAKEHOLDERS

- Stakeholders strongly supported the establishment of a unifying brand, identity and narrative for Canberra's cyber security ecosystem.
- Stakeholders suggested a national campaign to promote Canberra's cyber security capabilities to both cyber and non-cyber audiences.
- There was also strong support to form strong national and international partnerships with similar cyber security clusters around the world to collaborate on education, research and industry innovation.

3

CLUSTER ACTIVITIES (STEADY STATE)

- Establish a strong brand presence and reputation for the Cluster in the Australian and international cyber security landscape.
- Develop a strong online presence through the Cluster's website, online marketing and relevant social media channels.
- Establish a Cluster-branded and signposted physical 'Canberra Cyber Security Corridor' in the localities of key cyber security organisations.
- Promote and advocate for the collective capabilities of Canberra's cyber education, research and industry organisations.
- Establish partnerships with similar clusters in Australia and overseas.

4

CLUSTER ACTIVITIES (YEAR 1)

- Develop, launch and manage Canberra's cyber security brand and marketing strategy.
- Develop and manage co-branding partnerships with established organisations such as the Canberra Innovation Network and AustCyber.
- Promote and communicate Canberra's education, research and SME capability to national and international stakeholders through online, social media and traditional media platforms.
- Celebrate the successes of Canberra's education, research and SME organisations.

GOVERNANCE APPROACH

The Cluster will be underpinned by governance that will promote shared ownership

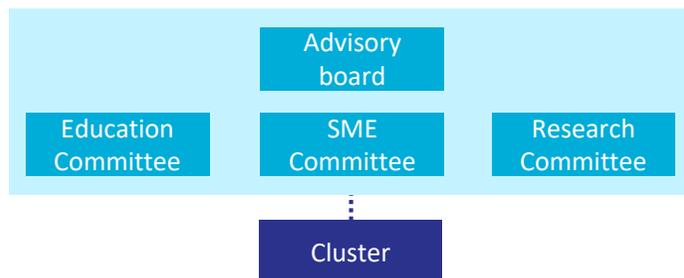
Stakeholders agreed that a model of shared ownership was essential to the success of any potential Cyber Security Cluster in Canberra. Key stakeholders must demonstrate commitment and contribute to the Cluster for it to be successful. It was agreed by the stakeholders that the governance and reporting structure of the Cluster should reflect this. While stakeholders voiced the need to have further clarity of the Cluster's objective and mission in order to design the governance model for the structure, they articulated key principles that the design should adhere to:

1. The Cluster must be an impartial and neutral body, and promote the collective interests and capabilities of its stakeholders, with open access to a wide range of cyber and non-cyber related organisations.
2. The Cluster must represent and include stakeholder cohorts that are likely to be affected by or benefit from the Cluster in decision making.
3. The Cluster must identify an initial funding source at the beginning to kickstart progress and the ACT Government should always remain a stakeholder.

Nous therefore suggests two governance options for Year 1 of the Cluster, with Option 1 being our recommended approach:

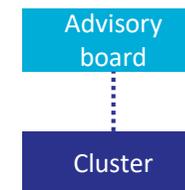
RECOMMENDED OPTION

OPTION 1: THEME-SPECIFIC COMMITTEES



All-of-cluster decisions are directed by a main advisory board, while theme-specific activities are directed by sub-committees made up of the most relevant stakeholder representatives. E.g. education pathway initiatives will be directed by an education committee, mainly made up of education provider representatives. Although more complicated, this structure allows for more focused decision making.

OPTION 2: SINGLE ADVISORY BOARD



All decisions are directed by a single advisory board with broad representation across education, SMEs and research. This structure is simpler but means that all board members are consulted for every matter that is brought to the board.

SECTION 3: CASE FOR THE CLUSTER

WHY CANBERRA?

Canberra is well positioned to be Australia's leading city for cyber security due its established ecosystem, proximity to federal government and concentrated footprint

Canberra is well positioned to be Australia's cyber security capital in response to Australia's cyber security policy, creating jobs and driving economic growth. It draws a natural advantage from being Australia's capital city with an established education, industry and government ecosystem where most of the government agencies, departments and influential policy makers are located. In addition, it has the following five differentiators:



Concentration of cyber security stakeholders

Canberra has Australia's highest concentration of Federal Government agencies, prime contractors, and small-medium enterprises engaged in cyber security. Federal Government agencies are collectively the second largest buyer of cyber security and together with organisations such as Northrop Grumman, Lockheed Martin and IBM, represent a significant concentration of cyber security buying power.

Established education and research capabilities

Canberra is home to three highly-ranked universities – ANU, UNSW Canberra and the University of Canberra; the National Computational Infrastructure (NCI); Data61 and CSIRO. These institutions collectively provide a concentration of cyber security research capability that is unmatched by other Australian cities.

Highly skilled, suitably security cleared workforce

Canberra has the most highly educated workforce and highest levels of workers with security clearances. This makes Canberra the ideal location to access a high-skilled talent cleared to access classified information and resources.

A highly networked business community

Owing to Canberra's small geographical foot print, Canberra's business, government, education and research stakeholders maintain strong relationships. This unique and connected network can be leveraged to deliver the multidisciplinary approach required for strong cyber outcomes.

Geographical proximity

Key cyber stakeholder, researchers, businesses and government departments are in close proximity within Canberra due to its small size. This has led to the formation of a natural "innovation corridor" within Canberra that delivers unique advantages for networking and collaboration.

WHY A CLUSTER?

A Cyber Cluster will provide the necessary scale, and a dedicated platform, for core stakeholders to access larger opportunities and stay ahead of competitors

Canberra has many strengths that already makes it the natural destination of choice for cyber security education and research. However, there are opportunities and threats to Canberra's cyber security economy that require collaborative effort.



Growing the ACT's collective share of the cyber security market

1

The Cluster can bring together 'competing' institutions and leverage their complementary strengths to grow the ACT's overall share of the cyber security market, therefore growing each stakeholder's share of the Australian cyber market. This will increase economic activity, create new jobs and develop sovereign capability within the ACT.

Addressing drivers of economic growth and opportunities that require collaborative effort

2

There are opportunities that cannot be addressed by any single party in the ACT cyber security ecosystem. These major opportunities require the coordinated actions of all parties, including responding to multidisciplinary or collaborative research opportunities and facilitating free flow of information between the various stakeholders. A Cluster has the potential to identify and address the economic gaps in the collective response of its stakeholders to broader market opportunities.

Competing with collaborative models emerging locally and overseas

3

There is a growing level of collaboration in the cyber security competitive landscape. These collaborations bring Canberra's cyber competitors' significant advantages, and stakeholders in Canberra risk losing out if it does not develop an effective model for collaboration to address this competition. We have provided examples of competing local and international clusters in the appendix.

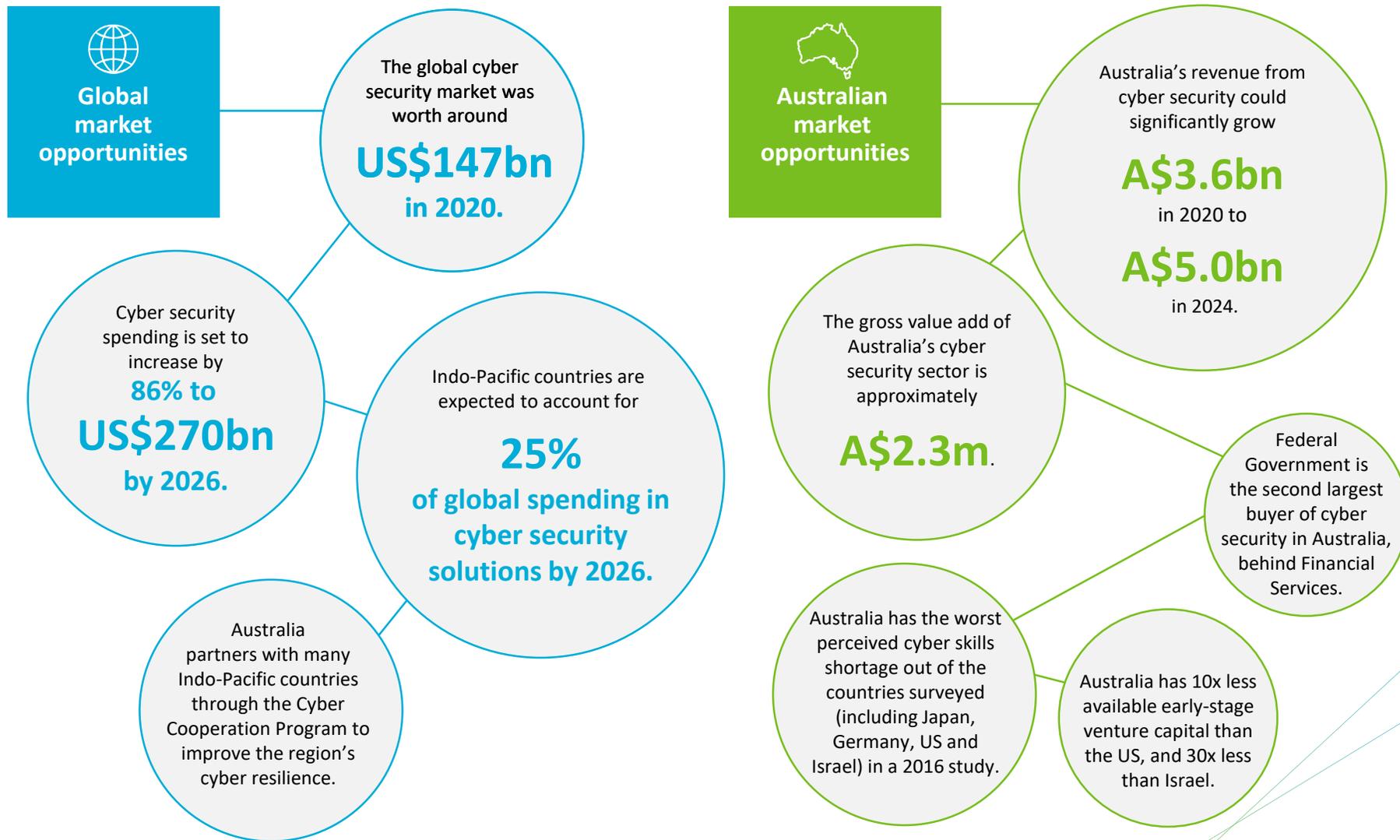
Simplifying an otherwise complex cyber landscape

4

The cyber security landscape is complex and can be difficult to navigate as a student, worker, business or investor. The Cluster has the potential to support buyers of cyber security education, research and services by providing them with a one-stop-shop (or shop front) for all cyber security matters in the ACT. This will reduce market frictions such as the lack of information to stimulate further economic activity.

WHAT IS THE MARKET OPPORTUNITY?

There is growing global and local cyber security market with key opportunities for Canberra to address



WHAT IS THE MARKET OPPORTUNITY?

Three key challenges and their influence on Australia's policy response present clear opportunities for Canberra to drive economic growth and create new jobs.

Australian policy is headed in the right direction but still requires concentrated focus and effort to overcome challenges shown below:



Sources: Australia's Cyber Security Strategy 2020, Australian Government; Australia's Cyber Security Sector Competitiveness Plan 2019 Update, AustCyber

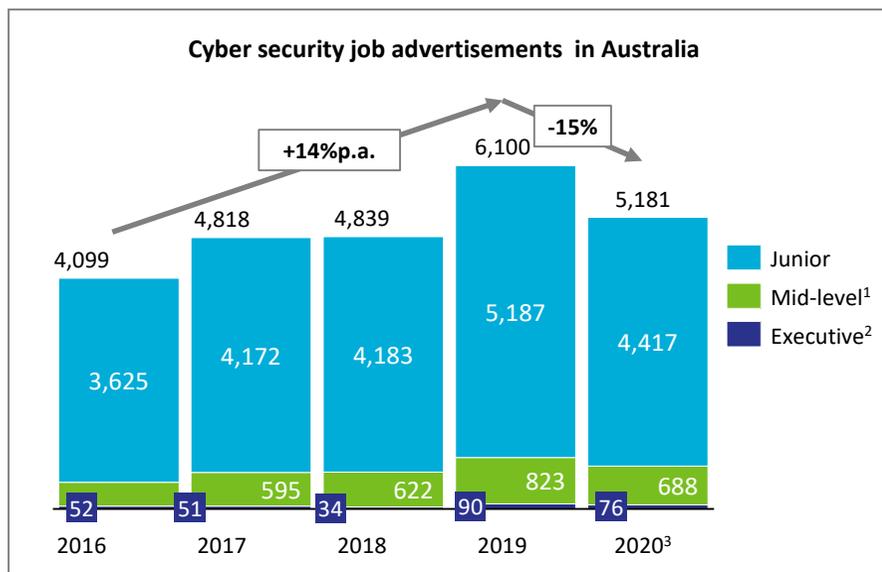
WHAT IS THE MARKET OPPORTUNITY?

Demand for cyber security jobs will continue to grow both in size and scope

There is evidence that demand in both specialist and cross-disciplinary skills are increasing consistently and these trends can be expected to continue.

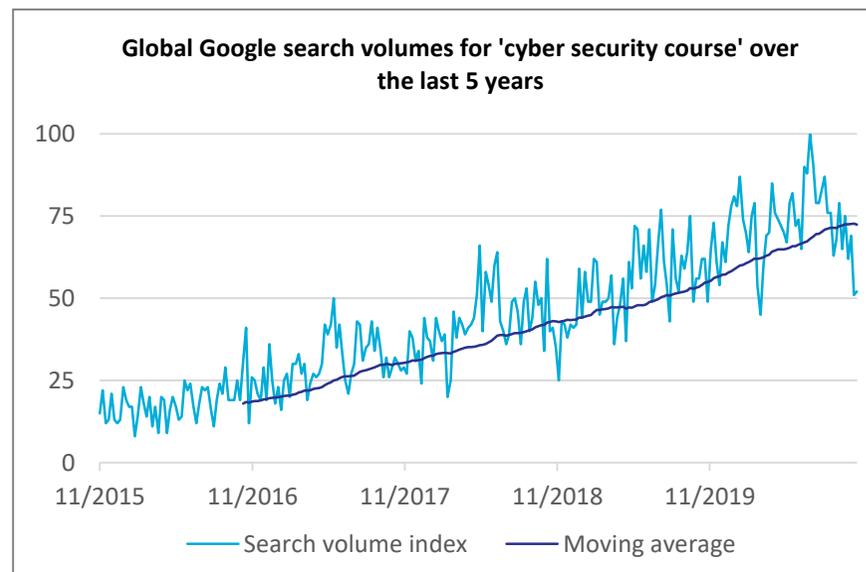
Cyber security jobs grew by 14% per annum up to 2019

In the four years from 2016 to 2019, cyber security job advertisements grew by nearly 50% overall. While COVID-19 has caused a dip in the market demand for cyber security jobs in 2020 (15%), cyber security jobs advertisements still outperformed those in professional, scientific and technical services, which declined by 18% on average in the same period. 2020 levels remain higher than any previous year except for 2019.



General interest in cyber security training and skills has tripled in the last five years

Google search volumes for key words relating to cyber security training and certification have increased consistently in the last 5 years. Volumes for some key words have tripled in this time with up to 10,000 searches (by unique individuals) performed in Australia each month. Globally, Singapore is the top origin and Australia is a top 10 origin for many related key words.



Notes: 1) Mid-level roles are defined as roles labelled as 'Manager' or 'Lead' which have typically more than 2 years of experience but not as senior as Executive roles.

2) Executive roles are defined as roles labelled as Director or C-suite level, typically with 10+ years of experience.

3) 2020 data is projected using YTD data, forecasted over the remainder of the calendar year.

Sources: Burning Glass ' Labor Insight™ Real-time Labor Market Information tool, [Nous Recovery Monitor](#), Google Trends, Google Keyword Planner

WHAT IS THE MARKET OPPORTUNITY?

Canberra has the potential to tap into an extensive array of Federal Government funding

There is a range of funding commitments that Canberra is well-placed to tap into through its higher education, research and vocational and technical education institutions. This will drive significant economic growth for the city and facilitate the creation of new jobs.

Investment of A\$1.67 billion by the Australian Government over ten years as part of its Cyber Security Strategy

The commitment is to achieve the vision of a more secure online world for Australians, their businesses and essential services. A core tenet of the strategy and funding is the equipping of governments, businesses and the community with the awareness, education and tools to be active contributors to the vision of a secure online world for Australians. Canberra has an opportunity to capture a significant share of the funding commitments shown on the right.

\$90m

to develop cybersecurity skills

\$67m

for critical infrastructure providers to enhance cyber capabilities

\$63m

to drive awareness and Australians and SMEs

\$1.6m

to enhance cyber security at universities

Emergence of cyber security related research grants and programs

The Australian Government and industry has developed a number of research grants and programs that have an exclusive focus on cyber, or identify it as a priority. With a diverse range of world-leading research capabilities covering theoretical, applied and commercial research areas through its three landmark universities, Canberra is in a uniquely advantageous position to bid for research funding through these grants and programs summarised on the right.

\$50m

Over seven years through the Cyber Security Cooperative Research Centre

\$400m

through the Defence Cyber Security Capability Improvement Program

\$64m

worth of cyber security research funding from the Federal Government between 2018 and 2020

Access to **\$2.4b**

in grants and programs that lists cyber security as a priority area

Sources: Australia's Cyber Security Strategy 2020, Australian Government; Australia's Cyber Security Sector Competitiveness Plan 2019 Update, AustCyber; 2016 Integrated Investment Program, Department of Defence; Research funding to address intelligence and national security threats, Office of National Intelligence; \$730 million fund for game-changing defence technologies, Department of Defence; National priorities and industry linkage working group; Department of Education Minister's Media Centre; Australian Research Council's Administration of the National Competitive Grants Program, Australian National Audit Office.

WHAT IS THE MARKET OPPORTUNITY?

Canberra can further develop its education offerings to better meet market demand

Canberra has the opportunity to develop a comprehensive suite of education pathways comprised of cyber-specific degrees, diplomas and certificates that mainly address demand for specialist cyber security skills; and majors, electives, short course that address the need for general capability and cross-disciplinary cyber skills.

The T-shape of cyber security skills

The skills that are required to meet future cyber security demands could be described as a T-shaped concept. The **vertical** bar of the 'T' represents the specialist and technical skills required in cyber security roles that are directly associated with cyber security including oversight, governance, assessment, protection, detection and response roles. The **horizontal** bar of the 'T' represents the general capabilities and cross-disciplinary cyber skills that executive, management, operations and other personnel need to play their part in enabling cyber security. This includes cyber-related analytics, complex problem solving, advanced communication skills and intercultural understanding.

General and cross-disciplinary

Specialist

A high-level review of Canberra's education pathways shows clear opportunities in the undergraduate and short-course space

Key: Area of key opportunity

	Australia National University	UNSW Canberra	University of Canberra	Canberra Institute of Technology	Other providers
Cyber security Masters / Doctoral Degree (AQF levels 9-10)	✓	✓			
Cyber security Bachelor Honours / Grad Certificate / Grad Diploma (AQF level 8)	✓	✓ (ADF only)		✓	
Cyber security Bachelor Degree (AQF level 7)		✓ (ADF only)			
Cyber security electives (as part of a IT or other degree)	✓	✓ (ADF only)	✓		
Cyber security Certificates, Diploma, Adv. Diploma, Assoc Degree (AQF levels 1-6)				✓	✓
Accredited cyber security short courses	✓ (Cyber law only)	✓ (ADF only)			
Non-accredited cyber security short courses		✓ ¹		✓ (Introductory course only)	✓ ²

Notes:

- UNSW Canberra provides 4 non-accredited short courses in cyber security spanning 15 subject areas across all levels. It also provides accredited micro-credentials which articulate into units of credit upon completion.
- There are multiple types of non-accredited cybersecurity short courses e.g. MOOCs provided across a range of different providers outside of traditional educational institutions

WHAT IS THE MARKET OPPORTUNITY?

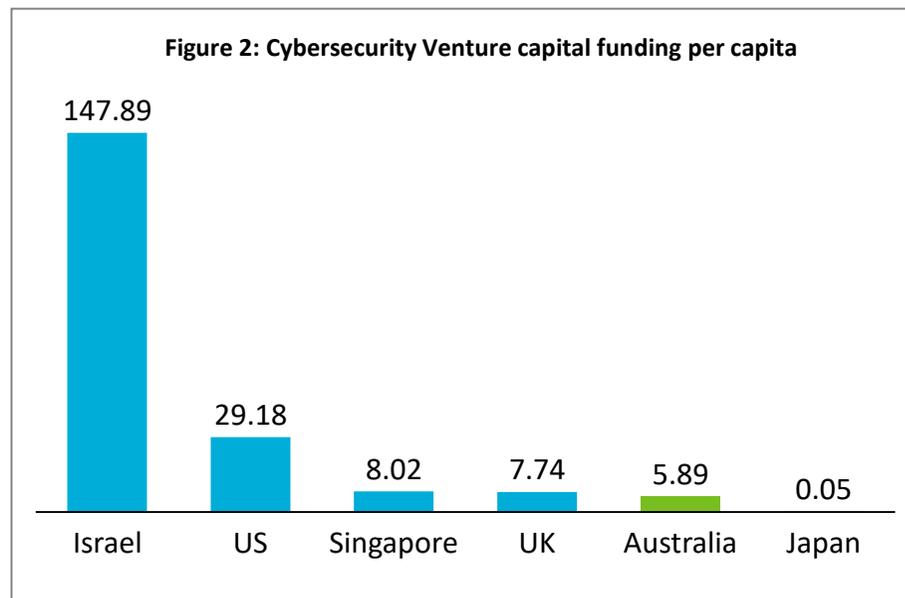
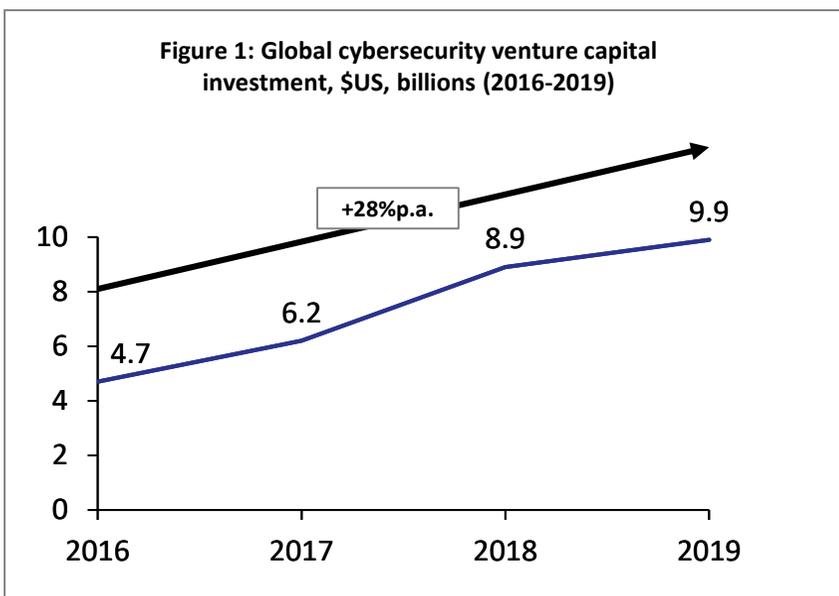
There is potential for cyber security businesses and start-ups to better attract the growing pool of foreign direct investment and venture capital and drive economic growth

Global cyber security venture capital investment grew by more than 28% per annum

Cybersecurity venture capital investment has more than doubled in size from ~\$US4.7B in 2006 to \$US9.9B 2019 globally. Investment has focused on cyber security organisations with SaaS-based models and automation capabilities, with growing emphasis on application security, micro-segmentation and authorisation.

However, the Australia's share of these funds has not been proportionate

Australia lags behind comparable economies in attracting cyber security investment. A notable difference between the VC environment in Australia and that of Israel and US is the absence of VC funds with expertise in cyber security. Indeed, AustCyber has already identified key opportunities for the Australian cyber security ecosystem to address including: improving information about funding, attracting foreign venture capital, vetting local organisations for funding and further developing cyber incubators and accelerators.



SECTION 4: A STAGED IMPLEMENTATION APPROACH

AN OVERVIEW TO THE IMPLEMENTATION APPROACH

The Cluster will begin as a virtual portal, with increasing presence, capabilities and physical footprint over three stages

Nous recommends the Cluster to be developed over three stages to deliver value early with minimal cost and risk while it is still reliant on ACT Government to facilitate and identify areas of seed funding. It will allow the Cluster to have clear milestones at the end of each stage, and realign its strategy for subsequent stages. The approach enables the Cluster to build its engagement and trust with stakeholders over time, enabling new collaboration and funding models to be developed as it progresses.

THE CONCEPT DESIGN FOR THE CLUSTER WILL DELIVER VALUE EARLY TO ENABLE MORE SOPHISTICATED COLLABORATION AND FUNDING MODELS TO BE EXPLORED IN LATER STAGES

Increasing brand presence

Increasing cluster capabilities

Gradual movement towards membership model

Decreasing reliance on ACT Government funding



Stage 1 (Year 1) Launch phase



Stage 2 (Years 2-3) Established brand



Stage 3 (Years 4+) Global reach

What are the guiding principles?

- Focus on areas that have strong support and are achievable
- Leverage partnerships and existing brands
- Low level commitment from 'partners'

- Explore models of collaboration
- Initiate flexible membership model
- Consolidate and build the cluster's own capabilities, assets and brand

- Develop sustained models for collaboration
- Establish tiered membership model
- Complete self-sufficiency

What form will the Cluster take?

An online portal connecting users to key education, SMEs, research and government partners

Stage 1 plus:
A physical 'Canberra Cyber Security Corridor' that is signposted with partner co-branding

Stage 2 plus:
Lead branding and presence across the 'Canberra Cyber Security Corridor', online and in media

What key activities will the Cluster undertake?

- **Promote and showcase** Canberra's education, research and SME capability
- Provide a **single doorway to education pathways** in Canberra
- Connect SMEs, industry, government and researchers through **networking events and a digital directory**
- Advocate for government procurement reforms to enable SME engagement

- Stage 1 plus:*
- **Grow** Canberra's education pathways
 - Develop an open **digital marketplace** to match relevant buyers, sellers and investors of cyber product and services
 - **Partner with similar cybersecurity clusters** in Australia and overseas
 - Facilitate development of **innovation sandboxes** at key organisations

- Stage 2 plus:*
- Develop **cyber-ready packages** comprising of local products and services
 - Explore **options for increased research** collaboration

What key enablers will support the Cluster activities?

- Budget and identify seed funding
- Co-branding and resources from key partners e.g. Brand Canberra, CBRIN, AustCyber
- 1-2 staff

- Initial seed funding (~50%)
- Non-compulsory member contributions (activity-based funding)
- 3-5 staff

- Ongoing seed funding (~20%)
- Membership fees on a tiered structure plus activity-based contributions from non-members
- 5+ staff

STAGE 1: LAUNCH PHASE

An online portal connecting users to key education, SME, research and government partners



What will this Stage cover?

Stage 1 of the Cluster will focus on activities that have strong support from stakeholders and can be implemented quickly.

The Cluster will focus primarily on the promotion of Canberra's education, SME and research capabilities. This will drive economic growth and create new jobs in the space. It will also facilitate connections between SMEs, industry and government by co-hosting cyber-focused networking events and publishing a digital directory of cyber organisations in the ACT. It will do this by leveraging the existing resources and brand equity of its partners such as ACT Government, the Canberra Innovation Network and AustCyber.

Importantly, this allows the Cluster to launch rapidly and deliver early value with a low level of commitment from the broader set of stakeholders.

What is the value proposition and for whom?

For education providers:

1. Increased exposure and referrals to prospective students and customers through the Cluster

For SMEs, research providers and employers:

1. Increased exposure and visibility of their organisation
2. Clarity of the key players in the Canberra cyber security landscape
3. Access to developing and developed cyber security talent

For prospective students and talent:

1. A single point of access for information about education and training options in the ACT

What promotion and branding activities will the Cluster engage in?

1. Develop, launch and manage Canberra's cyber security **brand and marketing strategy**
2. Develop and manage **co-branding partnerships**
3. Develop, launch and maintain the Cluster's **website**
4. **Promote and communicate** Canberra's education, research and SME capability through online, social media and traditional media platforms
5. Celebrate the successes of Canberra's education, research and SME organisations.

Year 1

STAGE 1: LAUNCH PHASE

An online portal connecting users to key education, SME, research and government partners



What activities will the Cluster undertake in education pathways?

1. Promote **existing education pathways** to prospective students and employers, providing clear information, advice and guidance (IAG)
2. Develop and launch a **virtual education portal** on the Cluster website to enable prospective students to learn about and navigate the education pathways in Canberra with ease
3. Conduct **initial analysis of industry, workforce and student needs** and facilitating development of new education and training offerings across the training needs spectrum (from specialist cyber security training to cross-disciplinary cyber offers) amongst education providers in the ACT
4. Facilitate identification and **development of work integrated learning**, student placement, internship, apprenticeship and graduate pathway opportunities for ACT education providers with industry and research partners

How will stakeholders be expected to engage with the Cluster?

1. Stage 1 will be a non-binding partnership model with no formal membership scheme in place
2. The public will have free access to the website and the full range of its features
3. Networking events will be open to the public and members of all organisations
4. Strategic partnerships with key stakeholders and organisations such as the key education and research providers, Brand Canberra, ACT Government, Canberra Innovation Network and AustCyber will be sought and managed

What activities will the Cluster undertake in accelerating SMEs?

1. Launch **networking events** that connect SMEs, start-ups, industry, government and researchers in collaboration with partner organisations
2. Publish a **directory** of cyber security SME and start-ups on the Cluster website to support discovery by potential customers and investors
3. Conduct **initial analysis** of industry cybersecurity innovation needs, government procurement priorities and approaches and provide recommendations to address barriers to entry
4. **Advocate for and facilitate improvements** in government procurement processes to address barriers faced by SMEs face in engaging with government clients

How will the Cluster be funded?

1. The Cluster will be funded by initial seed funding which will be identified and sourced
2. No membership contributions or fees are expected in Stage 1
3. The Cluster may seek corporate sponsorship from its strategic partners or other organisations and/or charge participants a small fee for networking events

What activities will the Cluster undertake in research?

1. **Showcase research successes** to date through articles on the website and media press releases
2. Publish a **directory** of research institutes and experts to facilitate discovery of Canberra's research capabilities
3. Analyse and share information on **collaborative research opportunities** with research providers

What resources will the Cluster need?

1. 1-2 staff FTE covering project management, business development, stakeholder management and branding and marketing capabilities
2. In-kind contributions from strategic partners including:
 - a) staff e.g. marketing, event management and IT
 - b) office and events space
 - c) digital infrastructure e.g. hosting servers, software licensing
3. Procurement of products and services for:
 - a) Marketing and communications
 - b) Events management
 - c) Website design and development

STAGE 2: AN ESTABLISHED BRAND

*An online portal
complemented with a
physical co-branded
'Canberra Cyber Security
Corridor'*



What will this Stage cover?

In Stage 2, the Cluster will shift its focus to explore models of collaboration between key stakeholders. The Cluster will also begin to consolidate and build its own capabilities and brand.

The Cluster will explore extending Canberra's education pathways to provide prospective students and customers with a comprehensive and compelling suite of education options. It will also leverage its connections with stakeholders and participants to develop a marketplace of buyers and sellers of cyber products and services, as well as sandboxes for collaboration and innovation.

To support its activities, the Cluster will begin to seek member contributions and activity-based funding from its strategic partners.

What is the value proposition and for whom?

For education providers:

1. Increased exposure and referrals to prospective students and customers through the Cluster
2. Growth and increased relevance in education offerings
3. Increased opportunity for revenue growth from additional students

For SMEs, research providers and employers:

1. Increased access to international buyers and investors of cyber security products and services
2. A comprehensive set of training offers with low barriers to address workforce needs
3. Access to developing and developed cyber security talent

For prospective students and talent:

1. A single point of access for information about education and training options in the ACT
2. Choice and flexibility in their learning options

What promotion and branding activities will the cluster engage in?

In addition to activities defined in Stage 1:

1. Establish a physical **'Canberra Cyber Security Corridor'** using co-branded signposting in the locality of key cyber security education, research and innovation organisations
2. **Celebrate** the Cluster's progress through government and industry co-branded events and communications.
3. Conduct **business development and advocacy** for the Cluster with prospective buyers or funders of cyber security innovation, education and research and employers
4. Form strong national and international **partnerships with similar cybersecurity clusters** around the world to collaborate on education, research and industry innovation

STAGE 2: AN ESTABLISHED BRAND

An online portal complemented with a physical co-branded 'Canberra Cyber Security Corridor'



What activities will the Cluster undertake in education pathways?

In addition to activities defined in Stage 1:

1. Collaborate with education providers to explore the potential to **extend Canberra's educational pathways** into growing areas such as micro-credentials and short courses
2. **Begin exploring recognition of programs** and units of study (both accredited and non-accredited) between different education providers in the ACT

What activities will the Cluster undertake in accelerating SMEs?

In addition to activities defined in Stage 1:

1. Conduct **regular analysis** of industry cybersecurity innovation needs, government procurement priorities and approaches and the needs of SMEs including interventions to address barriers to entry
2. Develop strong relationships and networks with **national and international clients and investors** e.g. Silicon Valley venture capitalists
3. Develop a preliminary membership structure for the Cluster including a tiering structure.
4. Launch a **digital marketplace** matching buyers, sellers and investors of cyber security products and services
5. Explore the development of collaboration and **innovation sandboxes** at key organisations e.g. large industry or government agencies

What activities will the Cluster undertake in research?

In addition to activities defined in Stage 1:

1. Develop a **shared understanding** of how the different research providers might leverage their individual strengths and niches to contribute to collaborative research

How will stakeholders be expected to engage with the Cluster?

1. Initiate flexible membership model in Stage 2
2. The public will have free access to the website and the full range of its features, including the marketplace
3. Networking events will be open to the public and members of all organisations
4. The Cluster will increasingly work directly with members and key stakeholders to explore the potential for sustained and scalable models for collaboration across education, industry and research
5. Strategic partnerships with key brands and organisations will be continue to be sought and managed

How will the Cluster be funded?

1. The Cluster will partly be funded by initial seed funding (approximately 50%)
2. No membership fees are expected in Stage 2
3. Non-compulsory contributions may be sourced from members and strategic partners or industry organisations for specific activities conducted e.g. development of an annual Canberra cyber security innovation report
4. The Cluster may continue to seek corporate sponsorship from its strategic partners or other organisations and/or charge participants a small fee for networking events

What resources will the Cluster need?

1. 3-5 staff FTE covering strategy, project management, business development, stakeholder management and branding and marketing capabilities
2. In-kind contributions from strategic partners including:
 - a) staff e.g. marketing, event management and IT
 - b) office and events space
 - c) digital infrastructure e.g. hosting servers, software licensing
3. Procurement of products and services for:
 - a) Marketing and communications
 - b) Events management
 - c) Website design and development

STAGE 3: GLOBAL REACH

An online portal complemented with a physical 'Canberra Cyber Security Corridor' led by a strong brand and presence of the Cluster



What will this Stage cover?

Stage 3 of the Cluster develop sustained models for collaboration between education, SMEs government, and research organisations.

The Cluster will leverage its progress to firmly establish partnerships with similar clusters and explore options for increased research collaboration within and beyond the Cluster. It will also develop and promote cyber-ready business packages comprising of local products and services.

Leveraging the Cluster's progress and its growing pool of stakeholders, the Cluster is now in a position to establish its membership model.

What is the value proposition and for whom?

For education providers:

1. Growth and increased relevance in education offerings
2. Increased global presence and reputation through world-leading education offerings
3. Increased international student numbers and revenue
4. Increased connection between education offerings, and work integrated learning and graduate pathways

For SMEs, research providers and employers:

1. Increased access to international buyers and investors of cyber security products and services
2. A comprehensive set of training offers with low barriers to address workforce needs
3. Access to developing and developed cyber security talent

For prospective students and talent:

1. A single point of access for information about education and training options in the ACT
2. Choice and flexibility in their learning options
3. Enhanced employment prospects

What promotion and branding activities will the cluster engage in?

In addition to activities defined in Stage 2:

1. Establish a strong **lead brand presence** across the physical 'Canberra Cyber Security Corridor', all digital and media channels
2. Maintain and leverage strong national and international **partnerships with similar cybersecurity clusters** around the world to collaborate on education, research and industry innovation

STAGE 3: GLOBAL REACH

An online portal complemented with a physical 'Canberra Cyber Security Corridor' led by a strong brand and presence of the Cluster



What activities will the Cluster undertake in education pathways?

In addition to activities defined in Stage 2:

1. Establish the **recognition of programs and units of study** (both accredited and non-accredited) across different education providers nationally and internationally

What activities will the Cluster undertake in accelerating SMEs?

In addition to activities defined in Stage 2:

1. Collaborate with industry and SMEs to **develop and sell cyber-ready packages** comprising of local products and services to national and international clients

What activities will the Cluster undertake in research?

In addition to activities defined in Stage 2:

1. Explore **options for increased research** collaboration across and beyond the cluster to attract large-scale funding opportunities

How will stakeholders be expected to engage with the Cluster?

1. A tiered membership scheme may be established in Stage 3, providing stakeholders with a range of membership options with different benefits and corresponding fee
2. The public will have free access to the website and the marketplace (as a buyer or investor)
3. Members have access to members-only website features such as listing a business, product or service on the marketplace
4. Networking events will be open to the public
5. The Cluster will work directly with key stakeholders to develop sustained and scalable models for collaboration across education, industry and research
6. Strategic partnerships with key brands and organisations will be continue to be sought and managed

How will the Cluster be funded?

1. The Cluster will continue to receive initial seed funding (approximately 20%)
2. The tiered membership structure will provide membership fees revenue
3. The Cluster will continue to seek non-compulsory contributions from strategic partners and industry organisations for specific activities conducted
4. The Cluster may continue to seek corporate sponsorship from its strategic partners or other organisations and/or charge participants a small fee for networking events (discounts may be provided to members)

What resources will the Cluster need?

1. 5+ staff FTE covering strategy, project management, business development, stakeholder management and branding and marketing capabilities
No change from Stage 2:
2. In-kind contributions from strategic partners including:
 - a) staff e.g. marketing, event management and IT
 - b) office and events space
 - c) digital infrastructure e.g. hosting servers, software licensing
3. Procurement of products and services for:
 - a) Marketing and communications
 - b) Events management
 - c) Website design and development

WHAT ARE THE NEXT STEPS TO IMPLEMENT THE CLUSTER?

Successful implementation of the Cluster will require attention in five areas

Nous recommends ACT Government to address the following areas to work towards the establishment of the cluster. The numbering of the five areas does not necessarily reflect the required order of execution. Some of these activities may be conducted concurrently.

1	2	3	4	5
Finalise the Cluster's mission, objectives and strategy with stakeholders	Confirm the Cluster's governance and reporting structures	Design and build the Cluster's stage 1 operating model	Project- and risk-manage Cluster development activities	Budget and identify the initial source for Cluster funding
ACT Government should 'close the loop' with stakeholders who participated in the workshop. This involves working with stakeholders to test and confirm the Cluster's mission, objectives and strategy to solidify their support and buy-in for Stage 1 of the Cluster design.	The form or type of entity of the Stage 1 Cluster will need to be determined and the necessary governance and reporting structures put in place to provide a clear operating framework. For stage 1, the Cluster could be managed as a separate project or as a BAU activity by dedicated personnel within CMTEDD. Reporting structures such as a steering committee or advisory group should be considered, as appropriate.	ACT Government should ensure there is a detailed design of the Cluster's stage 1 target operating model: people roles and capabilities, processes, technologies and strategic relationships that will support the Cluster's activities.	Robust project management will be required to ensure timely implementation of Stage 1, to navigate the associated issues and risks, and to continue engagement with the complex stakeholder landscape. A clear implementation plan with defined milestones, measures of success and stage gates should be developed, supported by a clear articulation of the risks and the mitigating strategies.	As discussed in previous slides, the Cluster will require initial seed funding. This will be budgeted and sourced. Finances associated with the Cluster should be forecasted and budgeted based on the target operating model and implementation plan, budget sources identified, and the necessary business case and approvals attained.

SECTION 5: APPROACH AND METHOD

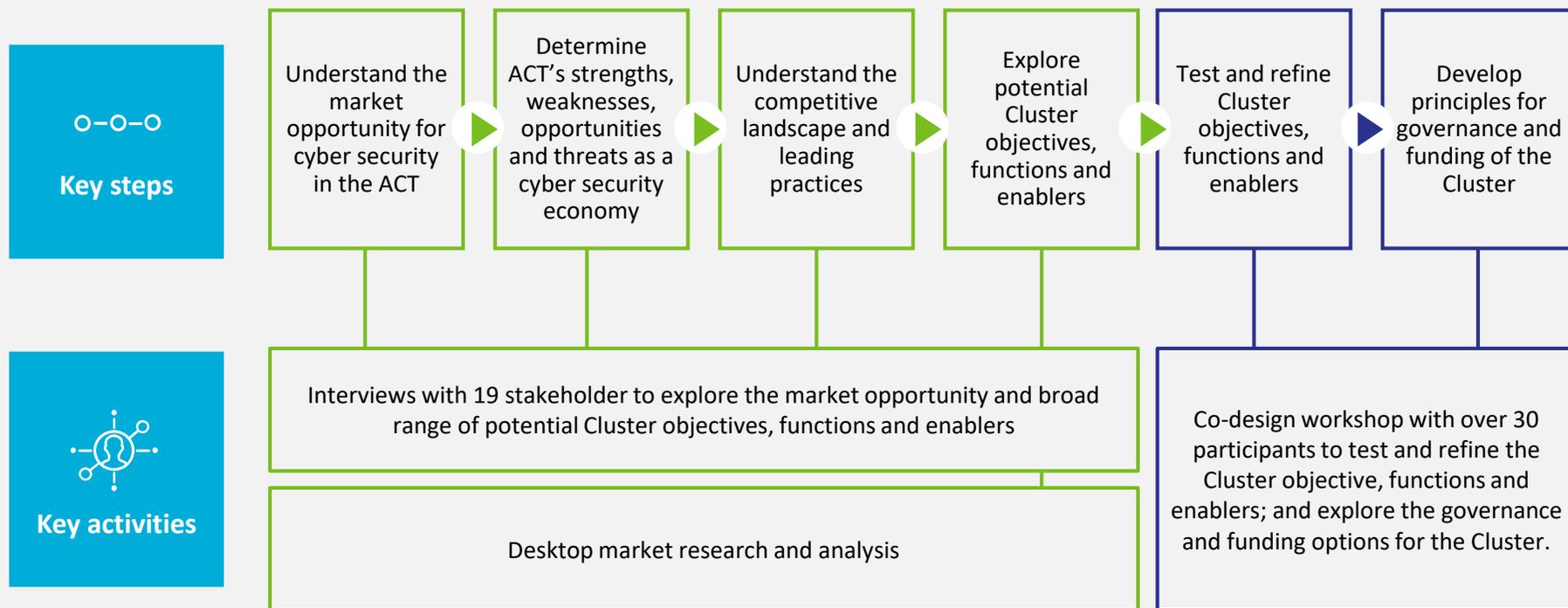
OUR APPROACH

Nous took a collaborative co-design approach to develop the Cluster model

Nous undertook a consultative approach to develop, test and refine the concept model for the Cluster. Nous engaged key stakeholders from ACT Government, education, research and industry organisations through a series of individual consultations and a co-design workshop. These consultations were further supported by desktop market research and analysis to create an evidence base for the broader market opportunities that the Cluster could address.

The diagram below provides an overview of the key steps and methods used to develop this report.

KEY STEPS AND ACTIVITIES OF THE PROJECT



WHAT DID WE HEAR FROM STAKEHOLDERS?

KEY THEMES EMERGED FROM OUR CONSULTATIONS AND CO-DESIGN WORKSHOP

Nous undertook a consultative approach to develop, test and refine the concept model for the Cluster. Initial consultations explored potential functions and activities of the Cluster. A broad range of ideas were provided by stakeholders. These are listed in the appendix. We synthesised these through further consultations and tested these key features at a co-design workshop. The below tables captures the key themes which emerged from the workshop, where participants drew consensus.

What did stakeholders say?

There is clear support for the Cluster with some functions taking priority over others.

- Stakeholders identified education and SMEs as the key priority areas for the Cluster as there were clear gaps and needs which could be immediately addressed. Conversely, there were complexities identified in research that should be explored at a later stage.
- Branding and promotion of Canberra and the Cluster should span across all three areas.

Stakeholders articulated some conditions for the success of the Cluster.

- The Cluster should be open to cyber and non-cyber organisations alike in Canberra and serve as an independent body.
- The Cluster should always have a clear and relevant mission and objective.
- It should leverage existing assets within Canberra before building new capabilities.

The implementation of the cluster should:

- Start small in both its size and scope
- Acknowledge that the cluster must build engagement and relationships to foster trust and goodwill with stakeholders over time.
- Deliver quick wins in Year 1 to prove the concept works e.g. start with 'one client' and build from there
- Initial funding should be identified to launch the Cluster and ACT government should maintain a stake in the Cluster over time

What are the implications for the Cluster?

- Given there are more compelling opportunities and less complexities in the Education and SME areas compared to research, the Cluster can immediately address these areas. Research opportunities will be explored at a later stage.
- Branding and promotion should initially be linked to broader, existing work to promote Canberra as a city before becoming more targeted e.g. to attract non-cyber organisations and new cyber sub-sectors to Canberra.

- Membership to the Cluster should not be financially restrictive. Any member fees should be commensurate to the benefit which the member receives from the Cluster. There should be a governance committee which represents the interests of the group e.g. working group or a steering committee
- The Cluster should remain specific to the needs of its members. There should be a realignment of the strategy at key points in its timeline e.g. throughout different stages.

- The Cluster should be implemented through a staged approach. ACT government should bear the initial risk and provide initial seed funding to incentivise stakeholders to engage with the Cluster without cost.
- As the Cluster develops, it should increase in maturity and become more self-sufficient and less reliant on government funding and resources.

HOW DID WE PRIORITISE CLUSTER FUNCTIONS AND ACTIVITIES?

We have assessed the range of potential activities within each function using three tests

Nous developed a series of tests to assess potential activities of the Cluster against the expectations and recommendations of stakeholders. These tests, shown below, incorporate the key considerations and requirements articulated by stakeholders during the consultation process.

Each of the potential activities being considered for the Cluster was assessed against these three tests to determine if it will be included in the Cluster design, when it should be implemented, and how it should be implemented.

THREE TESTS DETERMINE IF, WHEN AND HOW A POTENTIAL CLUSTER ACTIVITY SHOULD BE CONDUCTED BY THE CLUSTER

Is it desirable?

- Is there key stakeholder support for the activity?
- Is there a positive market opportunity that the activity will address?
- Is this opportunity not currently being addressed OR is there a gap?

Is it achievable?

- Is the proposed activity implementable?
- Noting the complexities and sensitivities of the activity, how easy is it to implement?
- Can the proposed activity deliver the intended benefits?
- Does the cluster have the capability to support the activity?

Will it complement existing capabilities?

- Is the proposed activity a unique activity that does not replicate or overlap with the functions of other stakeholder organisations?
- Can we leverage existing partnerships, capabilities and assets for the function?

SECTION 6: APPENDICES

STAKEHOLDER CONSULTATION LIST

We engaged with thirty six stakeholders throughout the course of the project.

Stakeholder engaged	Role
Adam Henry	Director, Fifth Domain
Alison Creagh	Defence Industry Advisory Board (DIAB)
Andre Diez de Aux	Senior Director, Policy and Strategy, ACT Govt
Andrew Muller	CEO - Ionize and Co-chair Canberra Node Industry Advisory Group
Anne-Louise Brown	Head of Corporate Affairs, Cyber Security CRC
Antony Hoskings	Director of the Research School of Computer Science, ANU
Ash Balarentnaraja	Executive Branch Manager, Skills Canberra, ACT Government
Bernadette Brown	Director, Cogito Group
Bettina Konti	Chief Digital Officer, ACT Govt
Daniel Baker	ACSC (Delegated by Abigail Bradshaw, CEO)
Dirk Pattinson	Director of Research ASD - ANU Co-lab
Geoffrey Crisp	Deputy Vice-Chancellor, Academic, University of Canberra
Hala Batainah	Chair, CBRIN
Ilsa Stuart	Senior Director Key Sectors & Investments, ACT Govt
Jade Demnar	ACSC (Delegated by Abigail Bradshaw, CEO)
Jason Chapman	Director of Operations, Quintessence Labs
Jayne Miller	Director - Business Growth and Transformation, CIT
Joe Lavery	Cybermerc

Stakeholder engaged	Role
Josh Bolton	Director, Defence and Intelligence, Penten
Kareena Arthy	Deputy Director-General, Chief Minister, Treasury and Economic Development Directorate, ACT Govt
Karen Jackson	Interim Lead, Commercialisation & IP, ANU
Kate Lundy	Defence Ambassador, DIAB
Kate Starick	Executive Group Manager, Economic Development Division, ACT Govt
Kris McCreath	Manager, Business Growth & Development, CIT
Linda Cavanagh	National Node Manager, AustCyber
Mark Tournier	A/g Director, Innovation, Industry & Investment, ACT Govt
Michael Frater	Rector, UNSW Canberra
Michael Callan	CEO, Australian Fraud and Anti-Corruption Academy
Michelle Fulton	Assistant Director, Key Sectors, ACT Govt
Mick Cardew-Hall	Pro Vice-Chancellor (Innovation), ANU
Nigel Phair	Director of Cyber, UNSW Canberra
Petr Adamek	CEO, CBRIN
Prerana Mehta	Chief of Ecosystem Development, AustCyber
Rachel Falk	CEO, Cyber Security CRC
Rod Kennett	Senior Manager for STEM Content, Questacon
Wanli Ma	Associate Professor, Information, Technology (IT) & Systems, University of Canberra

SUGGESTED CLUSTER ACTIVITIES FROM STAKEHOLDERS (1/2)

The comprehensive list of activities suggested by stakeholders are captured below

EDUCATION PATHWAYS

	1. Education pathways
	2. Accelerating SMEs
	3. Research
	4. Promotion and branding

Front-end activities

Provide prospective students and businesses with a virtual education portal that enables them to:

1. clarify their education and training needs
2. identify relevant pathways and learn how offers across different education providers in the ACT can be put together to meet their learning and career goals
3. learn about each offer, including work integrated learning and graduate employment opportunities
4. direct them to the appropriate providers and teams for further information and enrolment.

Back-end activities

1. Facilitating identification and development of work integrated learning, student placement, internship, apprenticeship and graduate pathway opportunities for ACT education providers with industry and research partners.
2. Development and maintenance of the virtual education portal.
3. Brokering recognition of programs and units of study (both accredited and non-accredited) between different education providers in the ACT.
4. Developing a roadmap for shared credit transfer regime amongst education providers in the ACT.
5. Conducting regular analysis of industry, workforce and student needs and facilitating development of new education and training offerings across the training needs spectrum (from specialist cyber security training to cross-disciplinary cyber offers) amongst education providers in the ACT.
6. Coordinate development of cyber security education for young people in primary and secondary education.

ACCELERATING SMEs

	1. Education pathways
	2. Accelerating SMEs
	3. Research
	4. Promotion and branding

Front-end activities

1. Provide service packages to SMEs and start-ups that may include:
 - a) access to a curated network of cyber security experts and stakeholders for business development and mentoring purposes
 - b) single-point of access to information services relating to cyber security grants, business supports, investors, incubators and accelerators
 - c) access to secure co-working spaces that are shared with other vetted SMEs and start-ups and in close proximity to established cyber security organisation and facilities
2. Provide access to cyber security data, research IP and infrastructure e.g. cyber sandboxes
3. Create and manage cyber marketplace to connect buyers and sellers of cyber security products and services.
4. Package and sell cyber-ready capability packages comprising local products and services to businesses in Canberra

Back-end activities

1. Regular assessment of the cyber security innovation needs and priorities of industry and government.
2. Regular analysis of Federal and other government procurement approaches.
3. Regular assessment of cyber security SME and start-up needs including barriers they face.
4. Development and management of service offerings for cyber and non-cyber businesses in collaboration with service delivery partners and cyber security stakeholders.
5. Developing a pipeline, assessing and vetting of cyber security SMEs and start-ups.
6. Development of access to innovation sandboxes at key organisations e.g. government agencies and large industry organisations
7. Client management and provision of services to SMEs and start-ups
8. Creating and maintenance of a database of cyber security investors, buyers and seller.

SUGGESTED CLUSTER ACTIVITIES FROM STAKEHOLDERS (1/2)

RESEARCH

	1. Education pathways
	2. Accelerating SMEs
	3. Research
	4. Promotion and branding

Front-end activities

1. Articulating the Cluster's research value proposition and capability offer
2. Development of business relationships with prospective Australian and foreign research funders.
3. Identification and development of collaborative research opportunities with Australian and foreign research funders.
4. Providing joint responses to relevant collaborative research opportunities on behalf of key research providers in the ACT.
5. Creating and managing a research marketplace for funders, buyers and providers of research capabilities.
6. Project managing delivery and liaising with external research stakeholders for collaborative research projects.

Back-end activities

1. Developing a shared understanding of how the different research providers will leverage their individual strengths and niches to contribute to collaborative research.
2. Analysis and sharing of information on collaborative research opportunities to research providers.
3. Coordinating and managing the collective response of research providers in the ACT to collaborative research opportunities.
4. Internal project management and coordination of research providers on collaborative research projects.
5. Providing critical research collaboration infrastructure such as research sandbox environments that are necessary for secure sharing of research resources.
6. Creating and maintenance of a database of research funders and buyers.

PROMOTION AND BRANDING

	1. Education pathways
	2. Accelerating SMEs
	3. Research
	4. Promotion and branding

Front-end activities

1. Marketing of Canberra's cyber security brand to prospective students, workers, businesses and investors.
2. Marketing and providing information on the Cluster, its objectives, value propositions, products and service offerings.
3. Providing information relating to the progress, opportunities and issues in the ACT cyber security ecosystem.
4. Business development and advocacy with prospective buyers or funders of cyber security innovation, education and research.
5. Advocacy of important matters in cyber security on behalf of ACT stakeholders.

Back-end activities

1. Development and management of Canberra's cyber security branding and marketing strategy.
2. Development and management of web, social media and traditional media presence in line with the marketing strategy.

ANALYSIS OF COMPARABLE CLUSTERS (1/2)

Five comparable clusters were identified and analysed against the ACT Government's objectives to identify learnings that could be applied to the Cluster. The two most comparable Australian cyber security clusters are highlighted below and overleaf with further case studies provided in the following sections.



Australian clusters

Oceania Cyber Security Centre (OCSC)

What is the context and objectives of the cluster?

The Oceania Cyber Security Centre (OCSC) was founded in November 2016 with the broad aim of engaging with industry, academia and government to conduct research, develop training opportunities and build capacity for responding to current and emerging cyber security issues locally and globally.

What form does it take, where is it and who are its members?

A physical cluster in Melbourne, Victoria. It has eight university members, two research centres and five cyber-related government and private agencies. These include: University of Melbourne, Monash University, Victoria University, AustCyber, AISA, Global Cyber Security Capacity Centre and more.

What functions does it perform?

The cluster publishes research through the associated think tank and research bank; conducts physical presentations; advocate for cyber security resilience

What progress has it made?

The OCSC has published its flagship assessment tool, the Cybersecurity Capacity Maturity Model for Nations (CMM). The tool helps assess five dimensions of cyber security and has been used by more than 80 countries to strengthen national cyber security capacity. Since starting the CMM program in 2018, the OCSC has conducted six CMM reviews within the Asia Pacific region with a further 9 scheduled in 2020-22, forming part of OCSC's outreach plan.

The OCSC is also a partner of the Global Forum on Cyber Expertise (GFCE), which is the global coordinating platform for cyber security building.

What lessons can Canberra learn from this cluster?

A focus on commercialisation of research has the potential to provide the Cluster with a revenue stream to fund its activities.

Australian Cyber Collaboration Centre (A3C)

What is the context and objectives of the cluster?

The Australian Cyber Collaboration Centre (A3C) was established in July 2020 in South Australia's innovation precinct, Lot Fourteen. It supports the development of a cyber workforce for global businesses that can establish cyber teams in South Australia to take advantage of world class research, education, and market reach in the region. It collaborates and shares ingenuity to innovate for improved future outcomes for private sector firms.

What form does it take, where is it and who are its members?

A physical cluster located in Adelaide, SA. It has a mix of industry, academia and federal / state governments including BAE Systems Australia, Optus, AustCyber, the Cyber Security Cooperative Research Centre, and the Defence Science and Technology Group.

What functions does it perform?

The cluster provides coworking space; organise networking events and activities; organise health activities; provide business mentoring and support services.

What progress has it made?

A3C houses the Cyber Training Academy and a Cyber Test Range, physical spaces for collaboration and cyber infrastructure to support product testing and training. This is used to carry out security testing of equipment or network configurations in the knowledge that networks are safe from interference. The Range is also used for certification, or standards-based testing to be performed.

What lessons can Canberra learn from this cluster?

The Cluster can generate a steady revenue stream to fund its activities by developing and providing a compelling cyber service offering that leverages its assets.

ANALYSIS OF COMPARABLE CLUSTERS (1/2)



Overseas clusters

Advanced Cyber Security Centre

What is the context and objectives of the cluster?

The Advanced Cyber Security Centre (ACSC) is the region's only non-profit, member-driven organisation to strengthen cyber security defences by bringing together the private and public sector and positioning members to be natural leaders in 'Collaborative Defence'.

What form does it take, where is it and who are its members?

It is a physical cluster based in Boston, Massachusetts. There are five university members (including Harvard and MIT), sixteen industry members and two government members

What functions does it perform?

The ACSC organises monthly roundtables and working sessions; organises an annual conference; and publishes research and newsletters.

What progress has it made?

The ACSC also established a biotechnology sector cluster to address the threats unique to the New England economy, attracting industry partners in Pfizer and Boston Scientific.

In education, it has formed an educational working group to improve curricula, promote internship opportunities, and increase the number of "job-ready" graduates.

What lessons can Canberra learn from this cluster?

The establishment of sector-based sub-clusters can directly address local market needs, as well as has the potential to attract and grow new or emerging sectors in the local economy.

North European Cyber Security Cluster

What is the context and objectives of the cluster?

The North European Cybersecurity Cluster (NECC) promotes cybersecurity-related collaboration in the Northern European region in order to enhance integration into the European Digital Single Market.

What form does it take, where is it and who are its members?

It is a virtual cluster with core members including the Norwegian University of Science and Technology, eight industry members and three government members.

What functions does it perform?

The NECC organises training, workshops, conferences; coordinate cybersecurity related projects and research; and promotes cyber security investment

What progress has it made?

The NECC hosts an annual Homeland Security Conference. This event brings together representatives industry, government and academia to share knowledge and strengthen capabilities around a common theme each year.

Last year, the NECC' introduced a new concept to pitch ideas and set up B2B meetings for new SMEs/start-ups to the cyber community.

What lessons can Canberra learn from this cluster?

Providing leadership in collaboration through regular events can help key stakeholders organise around and address current priorities in the ecosystem.

Cyber Security Cluster Bonn

What is the context and objectives of the cluster?

The Cyber Security Cluster Bonn aims to increase the sensibility and implementation of cybersecurity through practical informational offers, targeted at SMEs.

What form does it take, where is it and who are its members?

It is a virtual cluster with over 80 industry members including T-Mobile, Deutsche Post and DHL Group.

What functions does it perform?

The cluster promotes cyber-related study and training programs to the private sector and provides mentoring to IT security start ups. It also organises events, lectures and an annual summit.

What progress has it made?

The cluster has provided targeted coaching, mentoring, and financial support to local start-up organisations.

It has also provided the city and community of Bonn with secure digital technologies such as digital payment, autonomous driving, or secure digital access systems.

What lessons can Canberra learn from this cluster?

The cluster can leverage the assets and relationships of its members to be a cyber service provider or marketplace for local business and the community.

CYBERSECURITY JOB CATEGORIES AND KEY WORDS

These were the key words included in analysis of cybersecurity jobs advertised online.

Junior Roles		Mid-Level Roles	Executive Roles
Cyber	Splunk security	Incident Manager	Chief Security Officer
IDAM	ICT Incident	Cyber Security Manager	Chief Information Security Officer
Information Security	ICT Security	Security Product Manager	Chief It Security
IT Security	All Source analyst	Information Security Manager	Director Cyber
Penetration Tester	Mission Assessment Specialist	Security Controls Manager	Director IT Security
Security Analyst	Target Developer	Lead Security	Chief Cyber
Security Architect	Target Network Analyst	Lead Cyber	Director Information Security
Security Consultant	Exploitation Analysis	Principle Cyber	
Security Controls	Threat Analyst	Lead Penetration	
Security Designer	Partner Integration Planner	Lead Information Security	
Security Engineer	Network Engineer	IDAM manager	
Security Operations	Vulnerability Assessment Analyst	IT security manager	
Security Specialist		ICT security manager	
Signals Intelligence		Lead IDAM	

FEDERAL GOVERNMENT CYBER SECURITY STRATEGY 2020

FUNDING COMMITMENTS (1/2)

Measure	Expenditure
Cyber Enhanced Situational Awareness and Response (CESAR)	A\$ 1,350.0 million
- Assistance to critical infrastructure providers	A\$ 66.5 million
- Expanded national exercise program	A\$ 10.0 million
- Transformed Joint Cyber Security Centres	A\$ 67.9 million
- Enhanced customer engagement	A\$ 58.3 million
- Extend cyber security helpdesk for small businesses and families	A\$ 12.3 million
- Extend and expand offshore cyber crime disruption	A\$ 31.6 million
- Enhance cyber threat-sharing platform	A\$ 35.3 million
- New strategic mitigations and disruptions	A\$ 12.5 million
- Expanded data science capabilities	A\$ 118.0 million
- New national situational awareness capability	A\$ 62.3 million
- Emerging technology research labs	A\$ 20.2 million
- Australian Signals Directorate personnel	A\$ 469.7 million
- Intelligence capabilities and program administration	A\$ 385.4 million
Strengthening Australia's counter cybercrime capability	A\$ 164.9 million
- Bolster law enforcement capabilities	A\$ 124.9 million
- Establish a countering foreign cyber criminals capability with the ACSC	A\$ 40.0 million
Grow Australia's skills	A\$ 90.1 million
- Skills partnerships innovation fund	A\$ 26.5 million
- ACSC education and training programs	A\$ 6.3 million
- Data collection	A\$ 2.5 million
- Cyber skills for students and teachers	A\$ 14.9 million
- Grow the Defence cyber workforce	A\$ 40.0 million

FEDERAL GOVERNMENT CYBER SECURITY STRATEGY 2020

FUNDING COMMITMENTS (2/2)

Measure	Expenditure
Support to small and medium enterprises and vulnerable Australians	A\$ 63.4 million
- Expansion of Australian Cyber Security Centre's support to small and medium enterprises	A\$ 26.0 million
- Connect and Protect Program to assist SMEs with advice and assistance from trusted sources	A\$ 8.3 million
- Enhancing industry outreach and national capability collaboration	A\$ 8.2 million
- Cyber security awareness for Australian families, households and small businesses	A\$ 4.9 million
- Boost eSafety's investigations and support teams	A\$ 10.0 million
- Support to victims of cyber crime	A\$ 6.1 million
Enhance the cyber security of universities	A\$ 1.6 million
Total	A\$1,670 million

OTHER CYBER SECURITY PROGRAMS OR RESEARCH FUNDING

Measure	Expenditure
Cyber Security Cooperative Research Centre	A\$ 50 million over 7 years from 2018
Department of Defence Next Generation Technologies Fund which lists cyber research as one of nine priority areas	A\$ 730 million until 2026
Department of Defence Integrated Investment Program, which includes a Cyber Security Capability Improvement program	A\$ 400 million from 2016
Australian Research Council National Intelligence and Security Discovery Research Grant (NISDRG) which recognises cyber security as one of the eight intelligence areas of focus.	A\$ 18 million
Australian Research Council National Competitive Grants Program (NCGP), which recognises cyber security as a priority area.	A\$ 800 million in 2019-20
Federal Department of Education, Skills and Employment National Priorities and Industry Linkage Fund (NPILF) to support universities engage with industry and develop work integrated learning opportunities within STEM.	A\$ 900 million

CURRENT EDUCATION OFFERINGS BY HIGHER EDUCATION AND VOCATIONAL EDUCATION PROVIDERS IN CANBERRA

Institute	Course name	Type	Format
Australian National University	Cyber Security major within: - Bachelor of Advanced Computing - Bachelor of Information Technology - Bachelor of Software Engineering	Cyber security majors or electives	3-4 years full-time
Australian National University	Master of Cyber	Cyber security Masters / Doctoral Degree	2 years full-time
Australian National University	Graduate Diploma of Cyber	Cyber security Bachelor Degree / Graduate Certificate / Graduate Diploma	1 year full-time
Australian National University	ANU Ninian Stephen Cyber Law Program	Cyber security sub-degree	9.5 days
Australian National University	Graduate Diploma of Cyber Security, Strategy and Risk Management	Cyber security Bachelor Degree / Graduate Certificate / Graduate Diploma	1 year full-time
University of Canberra	Specialist major in Cybersecurity and System Administration within: - Bachelor of Information Technology - Bachelor of Software Engineering - Bachelor of Business Informatics	Cyber security majors or electives	3 years full-time
UNSW Canberra	Computing and Cyber Security (Honours) (Defence Force students only)	Cyber security Bachelor Degree / Graduate Certificate / Graduate Diploma	1 year full-time
UNSW Canberra	Computing and Cyber Security (CDF) (Defence Force students only)	Cyber security majors or electives	3 years full-time
UNSW Canberra	Bachelor of Computing and Cyber Security (Defence Force students only)	Cyber security Bachelor Degree / Graduate Certificate / Graduate Diploma	3 years full-time
UNSW Canberra	Master of Cyber Security	Cyber security Masters / Doctoral Degree	1 year full-time
UNSW (Online)	Master of Cyber Security (Online)	Cyber security Masters / Doctoral Degree	2 years part-time online
UNSW Canberra	Master of Cyber Security Operations	Cyber security Masters / Doctoral Degree	1 year full-time
UNSW Canberra	Cyber Security Boot Camp	Non-accredited cyber security short courses	5-day course
UNSW Canberra	Security Fundamentals	Non-accredited cyber security short courses	5 weeks (30 hrs total)
UNSW Canberra	Cyber Security Essentials	Non-accredited cyber security short courses	5 weeks (30 hrs total)
UNSW Canberra	Cyber Security Specialisation	Non-accredited cyber security short courses	5-day course
Canberra Institute of Technology	Graduate Certificate in Networking and Cyber Security	Cyber security Bachelor Degree / Graduate Certificate / Graduate Diploma	1-2 years part-time
Canberra Institute of Technology	Certificate IV in Cyber Security	Cyber security sub-degree	1 year full-time
Canberra Institute of Technology	Statement of Attainment training in Introduction to Organisational Cyber Security	Non-accredited cyber security short courses	Self-paced 9 weeks course

CURRENT EDUCATION OFFERINGS BY OTHER PROVIDERS IN CANBERRA

This list represents the cyber security courses on offer from the organisations we consulted throughout the course of the project. It is not an exhaustive list of providers in the ACT.

Institute	Course name	Type	Format
Cybermerc	Accelerated Cyber Analysis	Non-accredited cyber security short courses	1 week full-time
Cybermerc	Cyber Threat Intelligence - Foundations	Non-accredited cyber security short courses	1 week full-time
Cybermerc	Cyber Threat Intelligence - Advanced	Non-accredited cyber security short courses	1 week full-time
Cybermerc	Executive Cyber Risk	Non-accredited cyber security short courses	0.5-1 day full-time
Cybermerc	Executive Risk Identification	Non-accredited cyber security short courses	0.5-1 day full-time
Cybermerc	Executive Cyber Threat Management	Non-accredited cyber security short courses	0.5-1 day full-time
Ionize	Secure Coding	Non-accredited cyber security short courses	1 week full time
Australian Fraud and Anti-Corruption Academy	Diploma In Electronic Forensics	Cyber security sub-degree	30 weeks full-time
Australian Fraud and Anti-Corruption Academy	Certificate IV in Electronic Forensics	Cyber security sub-degree	21 weeks full-time
Australian Fraud and Anti-Corruption Academy	Electronic Forensics: Expert Witness Course	Non-accredited cyber security short courses	3.5 weeks full-time
Australian Fraud and Anti-Corruption Academy	Electronic Forensics: First Responders Course	Non-accredited cyber security short courses	9 weeks full-time