ADVANCED CYBER TRAINING CENTRE

FUTURE PROOFING AGAINST THE NEXT GENERATION OF CYBER ATTACKS.

PROSPECTUS

AN INVITATION TO HELP SHAPE THE SCOPE OF OUR FUNDING BID.

THE UNIVERSITY of ADELAIDE

THE UNIVERSITY OF MELBOURNE

UNSW

INTRODUCTION

Malicious cyber activity on Australian systems and networks are becoming ever more sophisticated, increasingly automated, and harder to detect.

In the 2020-21 financial year, the COVID-19 pandemic saw Australian businesses and households increase their use and dependence on the Internet. During this period, a cybercrime was reported every 8 minutes to the Australian Cyber Security Centre, with self-reported losses from cybercrime totalling more than $33 billion*.

The tactics and tools (known as tradecraft) of cybercriminals and state actors include complex technologies driven by artificial intelligence (AI) and machine learning, but also more familiar but equally devastating techniques like phishing and ransomware.

To address this issue, new thinking is needed about cyber hygiene. The proposed Advanced Cyber Training Centre will aim to develop and deliver on the new thinking required at a highly sophisticated level. Its mission will be not only to develop advanced technological solutions to cyber problems, but also to understand and integrate the human factors that make the cyber problems so complex in the first place.

WHAT MOTIVATES CYBERCRIMINALS AND STATE ACTORS?

Motivations	Emerging threats
Financial gain, corporate espionage	Threats to supply chains
Data and information theft for political reasons	Threats to IP
Cyber warfare	Political instability through influence operations
Personal information theft	Use of AI and quantum technology by malign actors
Notoriety and curiosity	Technology eroding human rights
	Disruption of critical infrastructure

* ACSC Annual Cyber Threat Report 2020-21, https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21

WHY A TRAINING CENTRE?

Australia's cyber research and training landscape

The Advanced Cyber Training Centre will differ to other cyber research collaborations, which typically focus on specific projects for individual businesses. Our centre will:

- provide the essential but currently missing training required by the cybersecurity industry, including by training already-established industry staff, and providing industry-driven research projects to promising PhD students
- be a longer-term relationship rather than a one-off research project
- build on lessons learned in other collaborations.

Emerging cyber threats will require a wider skill set than ever before. But there is a worldwide shortage of researchers with multidisciplinary cyber expertise such as cyber security, psychology, policy, AI, and ethical and legal literacy.

The global environment for advanced cyber experts is highly competitive with the US and China competing for global dominance. The Advanced Cyber Training Centre will help Australia capture a significant share of the cyber market and avoid the opportunity cost of not exploiting the technological leadership for which Australia's AI and machine learning sector is renowned.

Training for new roles in organisations, such as cyber leadership roles, will need to continually evolve. The Training Centre will create and stay on top of the latest knowledge and, as it will be led by the best universities in this field, will be strongly focused on producing and supporting high quality talent.

PARTNERS WANTED

"No sector of the Australian economy [is] immune from the impacts of cybercrime and other malicious cyber activity. Government agencies at all levels, large organisations, critical infrastructure providers, small to medium enterprises, families and individuals [are] all targeted... predominantly by criminals or state actors."

Australian Cyber Security Centre, 2021

We are seeking partner organisations to join us in a funding bid to the Australian Research Council across the whole cyber value chain.

These are just examples of potential partners, and interest from international partners is welcomed:

Cyber industry
Cyber equipment, technology and services (CETS) providers

End user (non-cyber) industry
Critical infrastructure operators (such as utilities, banks, telcos, data storage and processing providers) and users (including software providers and supply chain logistics companies), small to medium enterprises (SMEs), and education providers (including universities)

Government
Federal, state and local government organisations, including Defence, Police and Security

The Training Centre will be aligned with and positioned to respond to government plans such as the:

- SA Government Growth Sector Plans for Defence Industry and Hi Tech, and Workforce (skills and innovation)
- Department of Defence 2020 Defence Strategic Update & Force Structure Plan, and DSTG Information Warfare STaRShot.

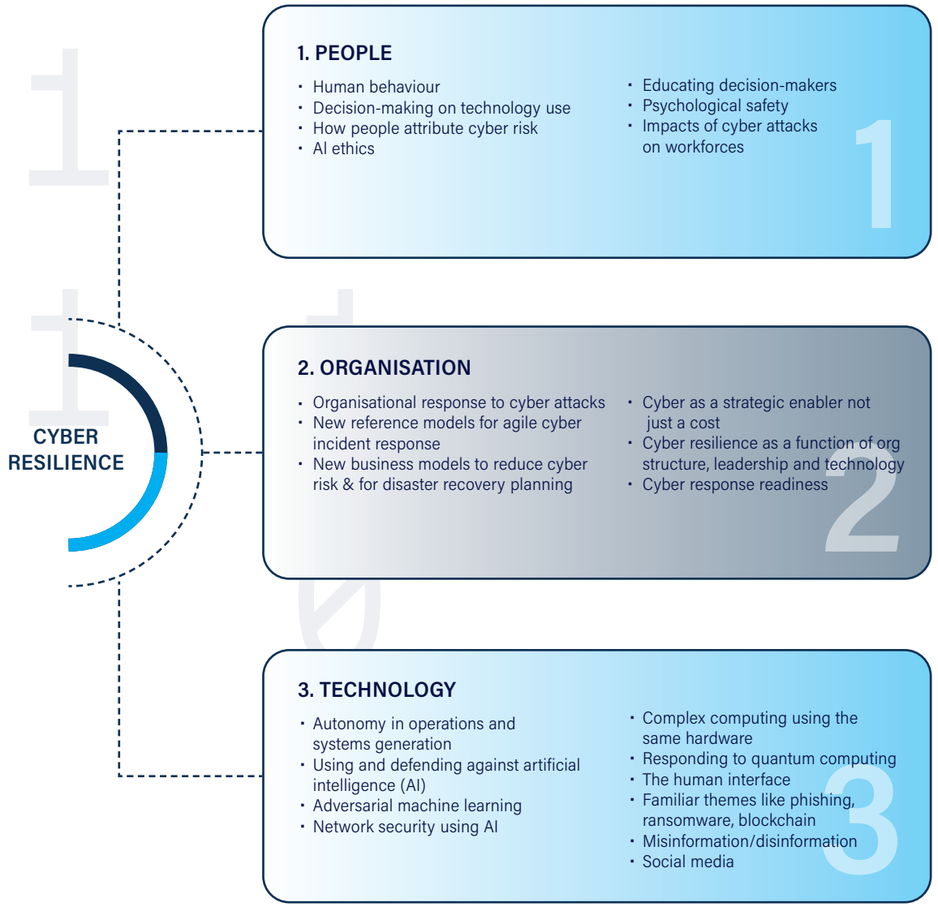
RESEARCH AND TRAINING SCOPE

The key question is: How can we rethink our systems and networks to be more resistant to attacks in the first place?

Advanced cyber is more than technology. It includes understanding threats and challenges arising from human behaviour and decision-making. The industry needs skilled people to analyse organisational cyber competencies and find gaps and solutions to raise their cyber hygiene level.

Goals

- Increase level of cyber resilience and hygiene in users and companies
- Develop a future-ready workforce with advanced cyber skills through PhDs and training
- Develop automated and adaptive defences against AI-enabled attacks
- Integrate a deep understanding of human cyberpsychology into defence systems
- Support the adoption of continually evolving technologies.



ABOUT ARC TRAINING CENTRES

The Australian Research Council (ARC) administers the Industrial Transformation Training Centres scheme, which fosters close partnerships between university-based researchers and end-users in industry and government. The goal is to create industry research capability and innovative solutions vital to Australia's future. Under the scheme, 'Training Centres' allow universities and their industry partners to secure matching funds to train the next generation of highly skilled people in industries important to Australia. They must address at least 1 of 9 Industrial Transformation Priorities, which include 'Cyber Security', and 'Defence'.

See the ARC Training Centres website for more:
arc.gov.au/grants/linkage-program/industrial-transformation-research-program/industrial-transformation-training-centres

How it works

- Industry partners lead the scope definition and co-design the research projects.
- The University of Adelaide applies for ARC funding to establish the Advanced Cyber Training Centre, up to a maximum of $5 million for 5 years. The proposal deadline is expected to be October 2022.
- At least 10 PhD students and 1 postdoctoral research fellow (that is, a researcher that has finished a PhD and is preparing for an academic career) are recruited.
- Industry partners co-supervise the PhD students, who are placed in industry workplaces for at least 12 months over the 5-year life of the Training Centre.
- Partners put in cash and/or other contributions such as staff time and access to facilities. The amount depends on the size of your organisation.
- Project findings may be published in the scientific literature and used to create content for university and industry courses for industry personnel, undergraduates and postgraduates.

R&D Tax incentive

Where sponsorship of the Advanced Cyber Training Centre is from an Australian entity it may qualify for a tax offset under the Australian Government's R&D tax incentive. The incentive provides up to 43.5% refundable tax offsets for eligible entities to encourage and support industry to conduct R&D.

See the Australian Government Business website for more:
business.gov.au/grants-and-programs/research-and-development-tax-incentive

PARTICIPATION OPPORTUNITIES

The Advanced Cyber Training Centre bid team is planning to request $4 million from the Australian Research Council (ARC). To be eligible and competitive for this funding, partners will need to make contributions.

Our goal is to raise $3 million in partner cash contributions: $1.5 million from industry and $1.5 million from universities over 5 years.

Tier	Investment requested	Benefits and responsibilities
Industry Level 1 - Large organisations	$250 k to $350 k cash in total over 5 years + in-kind	- Nominate 1 (one) representative on the Training Centre Steering Committee - Nominate specific projects for the Training Centre to work on (to be approved by the Steering Committee) - First rights to Intellectual Property (IP), to be defined in project agreements - Host 1 or more industry-PhD interns to work on your specific challenge (for 3 months per year over 4 years, on average) - Access to industry training that is continually updated in-line with the fast-moving research landscape - Access to network of Training Centre partners and other affiliations
Industry Level 2 - Medium and small organisations	$50 k to $100 k cash in total over 5 years + in-kind	
Industry Level 3	No minimum cash requirement + in-kind	- Host 1 or more industry-PhD interns to work within your organisation (for 3 months per year over 4 years, on average) - Access to industry training that is continually updated in-line withthe fast-moving research landscape - Access to network of Training Centre partners and other affiliations
University partner	$416,000 cash in total over 5 years + in-kind	- Nominate 1 (one) representative on the Training Centre Steering Committee - Nominate 1 (one) representative on the Science Steering Committee - Rights to publish innovative findings, to be defined in project agreements - Supervise and host at least 3 (three) industry-PhD interns (for 9 months per year over 4 years, on average) - Access to industry training that is continually updated in-line with the fast-moving research landscape - Access to network of Training Centre partners and other affiliations

BENEFITS TO PARTNERS

- Iterative **upskilling** for your practitioners
- **New staff** to develop products and services
- Talented students and researchers working on **your case study**
- Your university partners are established **world-class experts**
- **Stand out** from the crowd at the forefront of R&D
- Develop **next-gen products and services**
- New **tools, systems and networks**
- **Peace of mind** for you and your clients
- **Make decisions** about malicious cyber activity
- **Understand** your emerging threats
- **Networks** of researchers and end users

RESEARCH TEAM

Bid Leader

Professor Michael Webb
Director, Defence and Security Institute at The University of Adelaide

Michael is an experienced leader and award-winning researcher. He brings expertise in defence, mathematical psychology and cyber security to the leadership team.

University Partners

THE UNIVERSITY of ADELAIDE

Research under the Defence, Cyber and Space Theme at The University of Adelaide covers a full range of specialist physical, technological and computational capability. Researchers work closely with the university's award-winning Australian Institute of Machine Learning.

THE UNIVERSITY OF MELBOURNE

The Academic Centre of Cyber Security Excellence (ACCSE) at The University of Melbourne has an established program that includes industry PhDs working on industry problems, tertiary education and industry short courses. It brings together expertise from technical disciplines, law, and social sciences.

UNSW

The Institute for Cyber Security at the University of New South Wales specialises in multidisciplinary research, education, innovation, and commercialisation. In a unique research model, human and policy questions are embedded into projects and not an afterthought.

CONTACTS

BUILD TRUST WITH YOUR CLIENTS AND CUSTOMERS BY JOINING THIS INITIATIVE.

https://set.adelaide.edu.au/research-impact/defence-cyber-and-space

Professor Michael Webb
Bid Leader, and Director, Defence and Security Institute
The University of Adelaide
E: m.webb@adelaide.edu.au
T: +61 (0) 8 8313 0128

Associate Professor Toby Murray
Cyber Security Engagement
University of Melbourne
E: toby.murray@unimelb.edu.au
P: +61 (0) 3 8344 5080

Associate Professor Benjamin Turnbull
School of Engineering and Information Technology /
Canberra School of Professional Studies
University of New South Wales
E: benjamin.turnbull@unsw.edu.au
T: +61 (0) 409 342 050

July 2022- Version 1