



THE UNIVERSITY
of ADELAIDE

CYBER

An open invitation to partner
with the University of Adelaide

adelaide.edu.au



SECURING OUR DIGITAL FUTURE

Australia's democratic process is one of our greatest assets and most critical pieces of national infrastructure. Public confidence in it is an essential element of Australian sovereignty and governance.

But increasingly, it's under threat from cyber-attack—a fact brought into stark relief by 2018's malicious intrusion into the Australian Parliament House computer network.

The Australian Government has responded swiftly. Taking a proactive and coordinated approach, it has invested heavily in cyber security, including by expanding the Australian Cyber Security Centre (ACSC). The ACSC brings our country's Cyber capabilities together in a single place. This level of cooperation encourages the development and implementation of practical capacity- and confidence-building measures between states, and strengthens international cyber stability.

As a key ACSC member, the University of Adelaide fully appreciates that such collaboration is the best way forward. We've worked extensively with industry, government and the public to contribute our specialised Cyber capabilities and high-quality research in the past. And we're well placed to play a leading role in our nation's Cyber future.



We live in a highly connected world. The free flow of information within and between nation states is essential to business, international relations and social cohesion. But it doesn't take much to tip over into instability, or even chaos. We have become all too familiar with cyber-attacks on digital networks, and digital misinformation campaigns designed to degrade citizens' morale and wellbeing.

Cyber security is fast becoming a national priority, and the University of Adelaide is well prepared to help meet the challenge.

Our Cyber researchers' strategic insights and contextual intelligence allow us to explore, monitor and impact the global issues and forces driving transformational Cyber change. We're addressing the critical shortage of highly skilled Cyber professionals through new degrees, innovative training and internship programs, and industry collaborations, such as with Defence Science and Technology at Lot 14. Our world-class educators are equipping future leaders to influence and drive tomorrow's Cyber economy; and we're actively recruiting across borders to bolster the University and our state with additional outstanding Cyber talent.

We invite you to join us in securing our shared digital future.

PROFESSOR PETER RATHJEN, AO
Vice-Chancellor and President

The Cyber domain has become a ubiquitous feature of modern life. Products and services rely on it in almost every sector, meaning cyber security vulnerabilities now have an unprecedented capacity to compromise our society: from debate-changing fake news to identity theft and even major-infrastructure hacking, such as transport and financial systems, power grids and telecommunications.

At the University of Adelaide, we're committed to improving our nation's understanding of these threats and developing comprehensive and effective responses. Our holistic expertise encompasses human psychology and sociology, law and policy, computer science, and new developments in physics and engineering underpinning Cyber technology.

Above all, we recognise the importance of collaboration. Productive partnerships between research institutions, government and industry become more critical by the day; and we look forward to working with you to play our part.

PROFESSOR MICHAEL WEBB
Director – Defence, Cyber and Space

-
- 02** Meeting challenges from human to machine

 - 04** Human aspects

 - 06** Socio-cyber influence

 - 08** Cyber security

 - 10** Law and policy

 - 12** Cybercrime

 - 14** Cyber-physical systems

 - 16** Cyber in space

 - 18** Education and future workforce

 - 20** Engagement

 - 21** Let's collaborate

MEETING CHALLENGE FROM HUMAN TO



NGES MACHINE

As a globally engaged, world-class research institution, the University of Adelaide collaborates with industry and government to deliver high-impact, cross-disciplinary research across all aspects of Cyber.

Broad technological capabilities

Reflecting our mission to develop solutions to the security, privacy, reliability, trust and performance issues of different digital environments, we've built strong collaborative relationships between our researchers, industries and governments, both locally and internationally. Key among these, we're a core partner in Australia's Cyber Security CRC (Cooperative Research Centre).

Our research strengths include:

- intelligence analytics
- artificial intelligence
- cryptography
- blockchain
- digital forensics
- big data security
- human factors
- socio-technological security aspects
- privacy-enhanced technology
- trusted computing
- biometric security
- network security
- law and policy
- cyber security education.

KEY EXPERTISE AREAS



Human aspects



Cyber in space



Cybercrime



Law and policy



Cyber security



Cyber-physical systems



Education and future workforce



Socio-cyber influence

HUMAN ASPECTS

People are the weakest link in the cyber security chain, whether through malicious or non-malicious behaviours. At the University of Adelaide, we work closely with government, defence and industry to raise employees' cyber-risk awareness, and identify and implement best practice.

Collaborative behavioural research with DST

The University has partnered with the Defence Science and Technology Group (DST) for the past 10 years in the Human Aspects of Cyber Security (HACS) team. Supporting Defence and national security agencies, HACS engages with projects about human vulnerability to phishing, social engineering, employee compliance (with information security policies), and related cyber security fields. We conduct tests, experiments, surveys, interviews and focus groups with a range of partners, including Australian Government agencies, private industry and the general public.

Through this work we've co-produced a highly respected tool for measuring information security awareness—the *Human Aspects of Information Security Questionnaire* (HAIS-Q). Tested on over 6000 participants, HAIS-Q has featured in 18 external peer-reviewed publications, and has been used extensively in the Australian banking industry. It has also been adopted in several international projects, including in the UK, Netherlands and Indonesia.

Information systems research

Our Information Systems Research (ISR) team is a network of systems researchers with partnerships and alliances that target specific aspects of human cyber security and cyber safety. ISR's most prolific work to date has been with the Human Aspects of Cyber Security (HACS) team, but it also has significant secondary partnerships. These include with researchers from our: School of Education, investigating cyber security and cyber safety for children; and schools of Humanities and Social Sciences, exploring cyber security and cyber safety for senior citizens, the aging and elderly.

Future ISR partnerships are also planned to broaden the team's research into other sectors of society, ensuring a broad-scale, global approach to an increasingly critical worldwide problem.



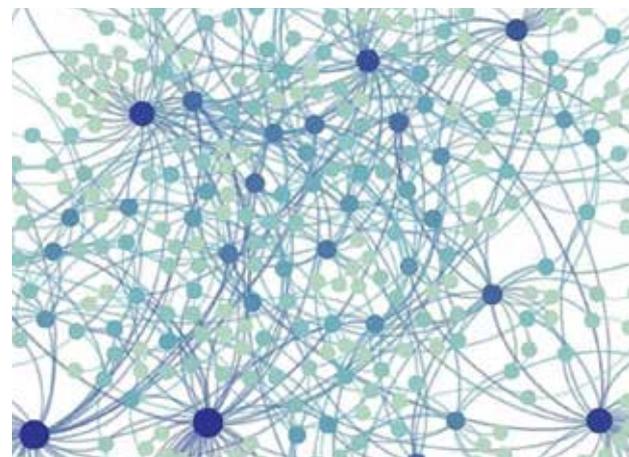
GRADUATE INDUSTRY PLACEMENT

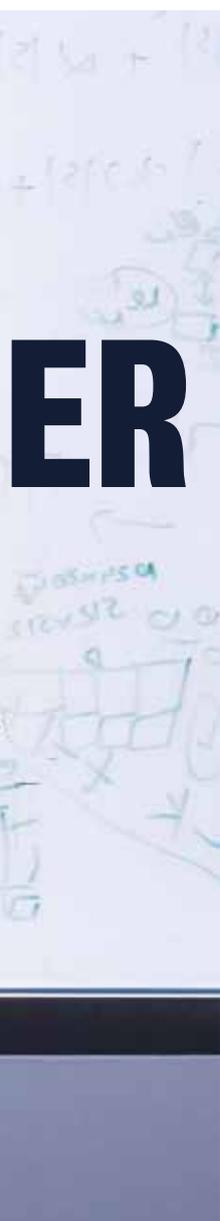
Candidates from our Master of Psychology (Organisational and Human Factors) work with DST's Human Aspects of Cyber Security (HACS) team on human vulnerability in cyber security fields. DST researchers hold adjunct research positions in the University of Adelaide School of Psychology, enabling supervision of honours, masters and PhD projects in the School of Psychology, linking graduates directly with industry.



SOCIO-CYB

This network shows a snapshot of social media conversations prior to a major public event. Nodes represent individuals; links represent Twitter mentions. Studying the network topology enables us to identify different classes of users (organisers versus advertisers), and by investigating messages' timing and content we can make inferences about information flow.





ER INFLUENCE

Based in our School of Mathematical Sciences, the Stochastic Modelling and Operations Research Group (SMORG) fuses theory, computation and data to address important and challenging problems affecting our world.

Studying the online to predict the offline

SMORG provides applied mathematical modelling, machine learning and data science expertise to illuminate numerous areas that are critical to Australia's cyber security and defence initiatives. These include:

- influence and information flow in social networks
- online social network analysis and modelling
- natural language processing, and particularly sentiment analysis
- artificial intelligence's predictability limits in complex socio-technical systems.

The team places particular focus on understanding human behaviours in online social systems, and how these may be used to predict offline behaviours and events. Among SMORG's recent real-world impacts, it has developed powerful event-prediction tools that use open social media data; these are now being incorporated in commercial forecasting applications for use by the Australian Government.

Biometrics and Video Analytics

The University of Adelaide is collaborating with DST to examine the utility of a collection of sensors for characterising individuals, and thereby facilitating people tracking, identification and assessment of mood. The project is also considering the exploitation of large-scale surveillance systems within which the biometric capability might sit.

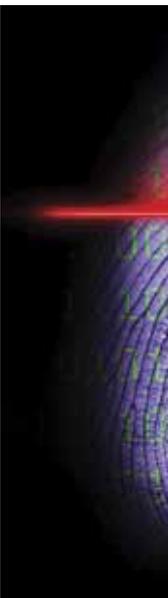
The project includes participation from the University of Adelaide's Schools of Medicine, Electrical and Electronic Engineering, Mechanical Engineering, Psychology, as well as the Australian Institute for Machine Learning (AIML).

With the initial focus of the biometric analysis being on gait, the project is now developing a more diverse collection of sensors and exploitation algorithms, and is looking to apply them in the wild (i.e. in weakly constrained environments, such as public spaces).

Collaboration with AIML has centred on an interest in large-scale CCTV networks, and on the cooperative exploitation of airborne and ground-based video sensors, an element of which involved data collection and participation in The Technical Cooperation Program's Contested Urban Environment exercise in 2017.

CYBER SECURITY

Researchers from our School of Computer Science, in partnership with CSIRO's Data61, are part of an international team that discovered the 'Meltdown' and 'Spectre' vulnerabilities in Intel processors made over the last two decades—issues threatening millions of computers, mobile phones and even cloud servers.



Enabling more secure processor design

The collaborative research team's work referred to above has been internationally recognised and reported. The *Meltdown* and *Spectre* 'bugs' exploit critical vulnerabilities in modern processors, potentially enabling hackers to steal passwords and other sensitive data through what are known as side-channel attacks. These discoveries will help to inform future processor designs, ensuring such threats are avoided.

Joining the University of Adelaide and Data 61 in the team are: Graz University of Technology, Austria; Cyberus Technology GmbH, Germany; and the University of Pennsylvania, University of Maryland, Google Project Zero and Rambus in the USA.

Our participating researchers' capabilities more generally include:

- microarchitectural attacks and countermeasures
- power and electromagnetic analysis
- side-channel cryptanalysis
- leakage-limiting system designs.



CYBER SECURITY COOPERATIVE RESEARCH CENTRE

The University of Adelaide is a key partner in the Cyber Security Cooperative Research Centre (CSCRC). Researchers from across six of our schools and three faculties help to shape the centre's programs, with four named research theme co-leaders. The CRC focuses on:

- ensuring critical infrastructure's security by developing innovative solutions to predict, prevent, detect and respond to cyber threats from nation states and individuals
- enabling industry and the community to access online services with confidence—enhancing Australia's reputation as a safe and trusted place to do business
- addressing workforce skills shortages by training the next generation of cyber security professionals.

Centre for Research on Engineering Software Technologies

Our Centre for Research on Engineering Software Technologies (CREST) researchers are experts in security-by-design. Using an interdisciplinary approach, they seek to inform the design, implementation and deployment of security- and privacy-preserving software-intensive systems and services.

The centre's research focuses on studying the causes, types and mechanisms of security challenges in software systems for cyber and cloud infrastructures. Some current projects include:

- Research Program in Tactical Information Resilience (RePTIR)
- Trustworthy Software
- Systems in Fog and Cloudlet Architectures
- requirement engineering for security
- automated data exfiltration detection and prevention
- middleware for managing data location, security and privacy
- collaborative workspaces for crowd-based design and industry-system validation.

CREST also actively supports future workforce development. For example, its researchers recently participated in a discussion panel on data-driven technologies for cyber security as part of Cyber Summer School, 2019—a joint initiative by Data61 and the DST.

Provable network security

Researchers from the University's Teletraffic Research Centre investigate novel methods for providing provable network security. Notably, they've developed a network configuration tool that models network policies in a metagraph, which automatically analyses and generates provably secure network configuration code.

The tool uses the rich formal foundations provided by metagraph algebra to visualise and analyse network policies' properties. From these formal analyses, it automatically corrects policy conflicts and generates network-level configurations that are provably correct.

When mature, the technology will provide the cyber security industry with a powerful, cost-effective and time-efficient method of:

- auditing network security configurations
- identifying policy inconsistencies, conflicts and non-compliances
- locating security configuration issues' root causes
- auto-generating provably correct and compliant network configurations from high-level policies.

LAW AND POLICY

Society's reliance on cyber capabilities has become pervasive. Security, privacy and policy issues abound. The University of Adelaide, through its Law School and School of Social Sciences, addresses many of the key emerging issues in Cyber.



The Adelaide Law School, through its Research Unit on Military Law and Ethics (RUMLAE), works on a range of legal issues arising in the cyber security environment.

Military legal and ethical issues

RUMLAE is an active participant in the Cyber Security CRC, where it plays a key role in multiple projects involving national security, data collection and privacy. These include:

- the use of de-identified information and the application of privacy law
- developing legal and ethical frameworks for data collection and sharing
- exploring legal and ethical issues in 'grey zones' and hybrid warfare
- the application of cyber security in the space environment
- addressing legal and ethical issues with the development and regulation of autonomous vehicles (including surface and air) and networked defence systems.

Illuminating criminological perspectives

Criminologists in the University's School of Social Sciences specialise in cybercrime, crime prevention, youth delinquency and policing. The research team is involved in various local, national and international projects, with key initiatives including:

- the Economic, Psychological and Societal Impact of Ransomware project, examining the human factors associated with ransomware deployment and victimisation (funded by the UK's Engineering and Physical Sciences Research Council)
- developing automated audio and facial recognition biometric tools for detecting child exploitation material (Commonwealth-funded)
- the Digital Youth Research Laboratory (see panel opposite).



Online networking protocols

Researchers in our School of Social Sciences have also redesigned fundamental online networking protocols in support of an alternative approach that favours security and autonomy over flexibility and ungoverned expansion. This broad research has implications across multiple fields, as it addresses basic cyber security and network governance problems plaguing IT departments and defence organisations worldwide.

DIGITAL YOUTH RESEARCH LABORATORY

The Digital Youth Research Laboratory (DYRL) is based at the University of Adelaide, with partners at Flinders University, the University of New South Wales, Michigan State University and De Montfort University. The DYRL team is involved in various research projects examining the links between how young people use technology, and pathways into—and out of—crime. Our work aims to inform public policy and promote safe and positive digital experiences.



CYBERCRIME

At the University of Adelaide, we're focused on leading digital security's exploration as an adaptive challenge, and increasing understanding of how it crosses industry boundaries.

Digital investigation

Researchers in our Faculty of Engineering, Computer and Mathematical Sciences (ECMS) conduct and prove cybercrime and digital forensic investigations for organisations all over the world, including providing expert-witness testimony in criminal cases to assist both police and Defence. Some of their current areas of focus include:

- digital image sensors' forensic identification, using sensor pattern noise, penetration testing, social engineering and advanced manufacturing technologies
- scientific validation of wearable sensors as forensic evidence
- image validation
- research in image and video provenance
- exploring the cybercrime implications of 3D-imaging technologies
- using dark current in CMOS image sensors as a unique identifier to assist with filtering online child exploitation or terror-related material
- developing knowledge in the investigation of cryptocurrencies and blockchain applications.



Raising Australia's digital-forensics profile

In 2008-09, our ECMS researchers founded the International Conference on Forensic Analysis and Techniques in Telecommunications, Information and Multimedia (eForensics). Then in 2018, the same group received a High Commendation for Developing Emerging Sources of Digital Investigation at the International Digital Investigation and Intelligence Awards.

Collaborative cyber security research program

A wide range of University of Adelaide Cyber researchers are involved in important domestic and international collaborations. These include:

- consulting to the South Australia Police (SAPOL) and the INTERPOL Digital Forensics Experts Group
- contributing to the UN Office on Drugs and Crime's Intergovernmental Experts Group on Cybercrime
- presenting at the International Communications Data and Digital Forensics conference in the UK with the London Metropolitan Police
- sitting on the (3-year, €7 million Horizon 2020) FORMOBILE From Mobile to Court project's scientific advisory board, hosted by Germany's Hochschule Mittweida university

- consulting on digital forensics to Estonia's Tallinn University of Technology (TalTech) and University of Tartu
- participating in the NATO Cooperative Cyber Defence Centre of Excellence
- consulting to the Australian Government's Department of Foreign Affairs and Trade
- contributing to the Adelaide Joint Cyber Security Centre, and its AustCyber cyber security innovation node.

Complementary education exchange

Since 2015, the University of Adelaide has offered a full-year program for research students—from honours to PhD—covering a diverse range of topics in cyber security and related applications, including eGovernment. This program includes an invaluable study tour and summer school exchange with students and staff from Estonia's Tallinn University of Technology and Germany's Hochschule Ravensburg-Weingarten.

Among the program's key highlights are:

- student presentations at an interdisciplinary cyber research workshop
- Internet of Things hackathon (Germany)
- meetings with industry, government agencies, military and academia in cyber security, eGovernment and entrepreneurship
- cyber security summer school hosted in Estonia, focusing on a different specific topic each year (in 2019 it was Blockchain applications and challenges).



CYBER-PHYSICAL SYSTEMS

Links between the cyber domain and the physical represent an important dimension to cyber vulnerability and opportunity. Advanced quantum devices and applied electromagnetics represent critical cyber-physical technologies that the University of Adelaide leverages to advance cyber capability.



ARC LIEF GRANT: EXPERIMENTAL IoT FACILITY

The University of Adelaide is a partner in an Australian Research Council Linkage Infrastructure, Equipment and Facilities (LIEF) grant. The grant will enable seven universities to establish a large-scale, real-world experimental facility for the Internet of Things (IoT). The University of Adelaide researchers will build a blockchain-enabled IoT infrastructure that is securely linked with the other six universities to make it a cyber range facility for evaluating the security of IoT applications.

Applied electromagnetic and antenna technologies

The University's Applied Electromagnetics Group undertakes a wide range of R&D activities for antennas and passive components at various frequencies—radio, microwave and millimetre-wave. A particular focus is placed on advanced antenna designs relevant for cyber, defence and related industries. The group's current projects include:

- designing antennas with frequency and polarisation agility
- conceiving shared-aperture antennas for multiple simultaneous functions, such as surveillance and agile communications
- integrating and/or concealing antennas in structures, vehicles and clothing
- developing frequency-selective surfaces able to alter objects' scattering response (e.g. thin radar-absorbing layers)
- creating advanced novel materials and additive technologies
- using computational and theoretical electromagnetics to accurately predict complex structures.

Multiple world-class facilities

Through partnerships with Silanna Group, DST and the CSIRO we've established an advanced R&D group specialising in quantum theory, device manufacturing and testing. With \$15 million in funding, the group's teams and state-of-the-art facilities include:

- our Institute for Photonics and Advanced Sensing (IPAS) Quantum Theory Group, exploring optoelectronic device quantum modelling
- the joint Silanna–University of Adelaide picoFAB MBE (molecular beam epitaxy) facility, including a Veeco three-chamber system for metal oxide production
- a joint DST–University of Adelaide MBE/microfabrication facility, including a Veeco single-chamber gallium arsenide system, enabling local development of high-power semiconductor laser diodes (a critical component of a cyber-physical defence against kinetic threats)
- our Adelaide Microscopy facility, providing TEM (transition electron microscopy) for materials qualification
- our IPAS Quantum Devices testing laboratory
- our Anechoic test chamber for devices.

Extending quantum-secured communications

Our IPAS Precision Measurement Group is using novel hollow optical fibres filled with laser-cooled atoms to create an efficient and long-lived quantum memory. This is the key piece of technology required to extend the distance of quantum key distribution in optical fibres, allowing for the development of a rugged and robust ground-based 'quantum internet' for provably secure information transfer.

The technology also has other crucial applications, such as supporting: creation of an optical quantum computer that could operate at room temperature; and development of new types of quantum simulators to probe the behaviour of quantum systems that are beyond current supercomputers' scope.



CYBER IN SPACE

The security readiness of the space industry, predicated by technology predating the modern Internet, is seen to be at a level ill-equipped to tackle the fundamental challenges posed by today's advanced adversaries skilled in technical and adaptive methodologies for attacking organisations.

Historically, space security has been assured by restricting access. Co-located missions open up the ecosystem to a variety of risks that have not yet been considered. An investigation on the need for secure small-form satellites using COTS components to enable multi-tenant missions while maintaining an acceptable level of mission risk from enemy vectors is needed.

Vulnerabilities of small-form factor satellites

The Defence Science and Technology Group (DST) has approached the University of Adelaide to conduct a cyber security and vulnerability assessment on their projected use of small satellites for co-located, multi-tenant missions. The primary focus is on the information and communications technology (ICT) subsystem and the way it could interact within a multi-tenant system. The ICT subsystem includes the electrical components of the satellite and ground stations, and the cyber security assessment includes the landscape of all electronic hardware. The University of Adelaide is leading the way in understanding critical areas of space security relevant to small-form factor satellites.

The University is also conducting research and development in global navigation system cyber vulnerabilities.

The findings have implications on establishing a security mindset within the Australian space industry, managing the adaptive challenge from frontline staff up to the executive level. This approach will assist space leaders with the adaptive challenge digital security poses in today's modern society.

SmartSat Cooperative Research Centre

The University of Adelaide's research leadership in artificial intelligence and machine learning for SmartSat systems, space situational awareness, advanced communications and electromagnetics, cyber security in space operations, and space law will provide key contributions to the SmartSat Cooperative Research Centre's research programs.

University centres involved will include: the Centre for Defence Communications and Information Networking; the Australian Institute for Machine Learning; Research Unit for Military Law and Ethics; and the Adelaide Applied Electromagnetics Group (AAEG).

The University of Adelaide Law school has membership in the Space Security Index Governing Council, and provides the application of cyber security in the space environment.

EDUCATION FUTURE WO

With more and more devices and systems connecting to the Internet, and cyber threats on the rise, employers increasingly seek graduates with advanced cyber security skills to digitally protect their customers and assets. At the University of Adelaide, we're providing them.



AND WORKFORCE

Shaping tomorrow's Cyber professionals

The University of Adelaide has an outstanding reputation for industry-oriented education, and collaborates closely with the private sector to produce high-quality, work-ready graduates with broad, applied knowledge. We're committed to fostering a security-aware culture, and to equipping our staff and students with the knowledge to thwart cyber threats.

Undergraduate opportunities

We offer a Cyber Security major in our:

- Bachelor of Engineering (Honours) (Electrical and Electronic)
- Bachelor of Computer Science
- Bachelor of Computer Science (Advanced).

Master of Cyber Security

Our Master of Cyber Security equips students to lead cutting-edge cyber security programs—for governments, law enforcement agencies, companies and NGOs alike.

The industry-driven content is delivered over 18-24 months full-time. There's a flexible blend of online and intensive on-campus learning, with mentoring from world-class cyber security researchers. Participants gain:

- a deep, interdisciplinary understanding of complex cyber security needs and considerations across multiple industries
- highly advanced technical skills and the ability to apply them in real-world contexts
- a sophisticated grasp of cyber security policy and governance considerations—social, legal and commercial
- the ability to critically analyse and evaluate relevant data and technology
- the refined interpersonal skills to effectively communicate issues and strategies to a range of stakeholders

Specialist courses are also offered in Cyber Security Management or Secure Software Development.

Research relationships

The University provides a wide range of options for government and industry to collaborate and supervise on, or sponsor, student research projects. We also encourage the support of scholarships and provision of internships. One of our key initiatives is with the DST at Adelaide's 'Lot 14' innovation and technology precinct, where we've partnered to develop a shared space for collaborative student research, including in Cyber.

GRADUATE CERTIFICATE OF CYBER SECURITY MANAGEMENT

The Graduate Certificate of Cyber Security Management is designed to meet the demand for cyber security managers in various sectors, including public, NGO, law enforcement and commercial. It provides a strong analytical and leadership framework to understand the challenges, problems and solutions of cyber security from a range of professional perspectives.

GRADUATE CERTIFICATE IN CYBER SECURITY (SECURE SOFTWARE)

The industry-driven Graduate Certificate in Cyber Security (Secure Software) content is delivered over six months, and prepares graduates to execute and manage cutting-edge cyber security programs in any sphere. It equips them with: a broad, manager's perspective on complex cyber security needs and issues; and a sound grasp of cyber security policy and governance considerations—social, legal and commercial.

GRADUATE INDUSTRY PLACEMENT

Candidates from our Master of Psychology (Organisational and Human Factors) work with DST on human vulnerability in cyber security fields. DST researchers hold adjunct research positions in the University of Adelaide School of Psychology, enabling supervision of honours, masters and PhD projects in the School of Psychology, linking graduates directly with industry.



ENGAGEMENT

The University of Adelaide is committed to working with government, industry and the wider community to link ground-breaking research with real-life applications, and make the transformative effect of a university education as accessible as possible.

By partnering with us, your organisation will gain opportunities to access innovative research, ground-breaking discoveries and the very best students—the sector’s next generation of leaders. We offer a broad range of engagement models and have decades of experience partnering with small and large organisations to deliver:

- multidisciplinary expertise at the centre of leading and emerging research
- access to world-class technologies and infrastructure
- dedicated organisational units, including the Institute for Photonics and Advanced Sensing (IPAS), Centre for Research on Engineering Software (CREST) and Australian Institute for Machine Learning (AIML)
- highly effective partnership models, including research strategy advice and support
- collaborative research leveraging third-party and government funding
- access to our national and global research partners, including our fellow Group of 8 universities and the DST
- access to University of Adelaide students through professional development programs, projects and our industry placement program
- customised and bespoke initiatives.

We look forward to working with you.

Government and industry strategic partnerships

The University has a proud history of collaboration with government and industry.

Key initiatives include:

- Collaboration with the DST on Adelaide’s Lot 14 precinct. We’re partnering to develop a shared space for collaborative, student-focused research.
- Participation in the South Australian Government’s Adelaide Cyber Collaboration Centre (AC3). Also located at Lot 14, AC3 will provide the opportunity to engage with various companies, AustCyber and the South Australian Government’s Office of Cyber Security.

We also have extensive experience in transitioning our research into high-impact practice.

Our national research centre participation

- Cyber Security CRC
- SmartSat CRC
- Defence CRC for Trusted Autonomous Systems
- ARC Centre of Excellence for Robotic Vision
- ARC Centre of Excellence for Mathematical & Statistical Frontiers
- ARC LIEF Grant: Experimental IoT Facility.

LET'S COLLABORATE

If your organisation could benefit from the University of Adelaide’s world-class facilities, resources or extensive research expertise, don’t hesitate to get in touch. We look forward to expanding our associations with industry and strengthening our nation’s Cyber capabilities.

In the first instance please contact:

PROFESSOR MICHAEL WEBB

Director – Defence, Cyber & Space

The University of Adelaide,
SA 5005 Australia.

Telephone: +61 8313 8261

Email: michael.webb@adelaide.edu.au

FOR FURTHER ENQUIRIES

The University of Adelaide SA 5005 Australia

 adelaide.edu.au/cyber

 facebook.com/uniofadelaide

 twitter.com/uniofadelaide

 snapchat.com/add/uniofadelaide

 instagram.com/uniofadelaide

© The University of Adelaide.
Published July 2019 3861-7
CRICOS 00123M

DISCLAIMER The information in this publication is current as at the date of printing and is subject to change. You can find updated information on our website at adelaide.edu.au or contact us on 1800 061 459. The University of Adelaide assumes no responsibility for the accuracy of information provided by third parties.