RMIT Centre for Cyber Security Research and Innovation

Five Year Impact Report

RMIT UNIVERSITY

Centre for Cyber Security Research and Innovation

Foreword

Congratulations to the RMIT University Centre for Cyber Security Research and Innovation (CCSRI) on reaching the milestone of five years since its establishment.

Over the past five years the work of the Centre has closely aligned with the strategic direction of the RMIT College of Business and Law, RMIT College of Science, Technology, Engineering, and Mathematics, and the wider University through its multi-disciplinary, impact-driven approach to research and education. CCSRI's mission to deliver real-world solutions to cyber security challenges through in-depth collaboration with industry, government, and academia reflects the College's commitment to applied research and industry engagement. The Centre operates at the intersection of technology, business, and social impact, aiming to address pressing global cyber security issues with innovative, evidence-based strategies.

CCSRI's focus on the organisational, human, and technological dimensions of cyber security supports the College's strategic position as a leader in business and technology education. The Centre's work in shaping policy, enhancing cyber resilience, and protecting the Australian community through cyber security innovation complements the College's purpose of creating and disseminating knowledge that informs ethical and sustainable business practice. This synergy is particularly evident in CCSRI's award-winning education projects and its international footprint, including its hub in Vietnam and its work in the Baltic region.

Furthermore, CCSRI's contributions to RMIT's broader "Knowledge with Action" strategy, particularly in the areas of emerging technologies and social innovation, demonstrate its integral role in advancing the University's vision for inclusive, sustainable futures. By mobilising expertise across Colleges, disciplines and geographies, CCSRI both enhances the College's research profile and supports its goal of preparing government, industry and academia to shape the future responsibly.

As CCSRI prepares for the next five years of advancing cyber security and resilience in Australia and beyond, its efforts will remain focused on addressing complex cyber challenges in the rapidly evolving digital and economic landscape.

Professor Colin Picker
Deputy Vice-Chancellor Business and Law and Vice-President
RMIT University

Acknowledgement of Country

RMIT University acknowledges the Wurundjeri people of the Kulin Nation as the traditional owners of the land on which the University stands. RMIT University respectfully recognises Elders both past and present.

Acknowledgement

The RMIT University Centre for Cyber Security Research and Innovation acknowledges with deep respect the passing of Professor Darius Štitilis in March 2024. Professor Štitilis, Dean of the Faculty of Public Governance and Business at Mykolas Romeris University, Lithuania, served as founding member of the Australian Lithuanian Cyber Research Network, providing exceptional leadership and insight. His contributions to advancing cyber security research in Lithuania and the Baltic region have left a lasting legacy for both our institutions and for the broader academic community.

Contents

1 CCSRI Director's Introduction

> "The Centre adopts a multi-disciplinary approach to cyber security research and innovation and continues to strengthen its engagement with industry and government to build a more cyber secure and resilient Australia."

From its establishment in 2020, the RMIT University Centre for Cyber Security Research and Innovation has pursued a multi-disciplinary and applied approach to research, education and innovation in cyber security, with in-depth consideration of the human, organisational and technological aspects of the field.

Our mission has been to create tangible impact and real-world solutions with an integrative approach to cyber security as a leading source of research and innovation in both Australia and overseas.

To achieve the Centre's mission and vision we have brought together a team of experienced researchers who look at cyber security from a truly multi-disciplinary perspective. These academics and researchers are drawn from RMIT University's College of Business and Law, College of Science, Technology, Engineering and Mathematics, and the College of Design and Social Context. The Centre also works closely with industry bodies and practitioners as well as government agencies, both in Australia and internationally, to investigate and address cyber security issues, challenges and opportunities and advance the field of cyber security.

This report showcases just some of the exemplary cyber security research and education projects that these academics and researchers working alongside our industry and research partners have undertaken. These projects have created meaningful impact across a diverse range of areas, with a focus on addressing the cyber skills gap in industry and across communities, securing Australia's critical infrastructure, strengthening Australia's defence and national security, forging international collaboration and partnerships, and exploring new boundaries in cyber security.

Looking forward, in the next five years the Centre will continue to explore new interests and areas of multi-disciplinary research and innovation into the organisational, technological and human aspects of cyber security, working to advance cyber security and resilience both within Australia and globally, through active engagement with industry and government partners.

Professor Matthew Warren
Director, RMIT University Centre for Cyber Security Research and Innovation

2 CCSRI Research Overview

> “The Centre’s breadth allows us to address not only the technical dimensions of cyber security but also the human, regulatory, and organisational challenges that shape national resilience. We continue to deepen our partnerships with industry and government, ensuring that our research translates into practical solutions and informed policies that strengthen Australia’s cyber capabilities and contribute to a safer, more resilient digital future.”

The mission of the RMIT University Centre for Cyber Security Research and Innovation (CCSRI) is to be acknowledged—both nationally and internationally—as a world-class centre in multi-disciplinary cyber security research. Since our launch in July 2020, CCSRI has delivered impactful research and forged substantial collaborations. We have led major successful large-scale initiatives, such as the A$1.6 million federal cyber security project in collaboration with the University Foreign Interference Taskforce (UFIT), focusing on threat modelling and intelligence sharing across Australia’s higher education section. We have also been actively involved in the A$13 million ARC Research Hub on digital manufacturing, which involves major Australian universities and large manufacturing companies to grow and accelerate Australian digital manufacturing (DM) transformation by devising novel DM technology and commercialisation/adoption pathways.

Our researchers are at the forefront of innovation, winning several industry, research, and education awards, including competitive ARC (Australian Research Council) grants (e.g. ARC Discovery and ARC Linkage), ARC LIEF (infrastructure grant) and CRC-P. CCSRI members also publish in prestigious conferences and journals, such as Security & Privacy, ACM Conference on Computer and Communications Security, and Network and Distributed System Security.

Our success is underpinned by strategic and strong partnerships with local industry and other research organisations (e.g. CSIRO). This includes close collaboration with the Sir Lawrence Wackett Defence and Aerospace Centre (led by Prof Pier Marzocca), and a robust Cyber Industry Advisory Board comprising cyber professionals and executives who guide both our research direction and engagement strategies.

Looking ahead, CCSRI’s focus will extend to securing emerging domains such as AI security and privacy, quantum computing, and critical infrastructure, while addressing human factors, governance, and resilience in complex digital ecosystems. We will continue to drive impactful, cross-disciplinary collaborations that translate rigorous research into deployable solutions, shaping cyber policy and practice both nationally and internationally. Above all, CCSRI aims to play a pivotal role in developing the knowledge, technologies, and a skilled workforce to safeguard Australia’s digital future.

Professor Zahir Tari
Research Director, RMIT University Centre
for Cyber Security Research and Innovation

3 CCSRI Contributions to the Cyber Security Environment

Australia's critical infrastructure underpins the entire knowledge economy, including government, organisations, defence, law enforcement, and emergency services. But Australia's critical infrastructure is vulnerable to cyber attacks by malicious actors and is subject to damage caused by non-malicious events such as natural disasters, equipment failure, human error, and other accidents. It is essential that the security and resilience of Australia's key infrastructure be assured, it shows that cyber security is critical to the future of Australia.

Cyber security continues to be one of the top areas for investment in Australia's strategic research priorities. However, in Australia there is a critical shortage of suitably trained and qualified cyber security professionals, and current investment does not match the magnitude of the problem.

In recent years, the rapid development of artificial intelligence (AI) and its widespread adoption presents opportunities in addressing workforce challenges and organisational efficiencies, but also raises concerns about cyber security implications and the potential for misuse, such as through scams and disinformation.

Addressing these cyber security challenges requires a concerted effort from all stakeholders and countries to develop and implement effective solutions. The Australian Government in 2023 invested $4.2 billion via the *2023-2030 Australian Cyber Security Strategy*, which took a holistic approach for government, industry and academia to enhance cyber security, manage risks and support Australian citizens and businesses in navigating the cyber environment.

Since its establishment in 2020, CCSRI's research and innovation initiatives have consistently aligned with industry challenges, government strategies, and have a forward-looking focus on cyber resilience, as demonstrated in the case studies within this report.

As recognition of this alignment, CCSRI has been privileged to win several industry, research and education awards, including:

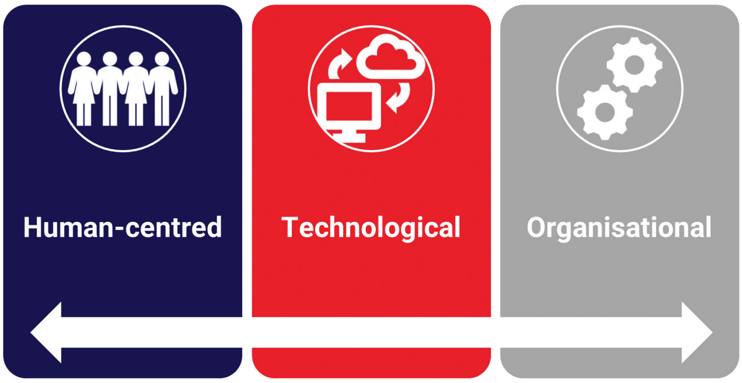
- VNISA (Vietnam Information Security Association) Award (2025) –for the Cyber and Critical Technology Cooperation Program industry training.
- VNISA Certificate of Merit (2023) – for outstanding contributions to VNISA.
- AISA (Australian Information Security Association) Best Researcher of the Year Award (2023) – for the Gender Dimensions in the Australian Security Industry project.
- iTnews Benchmark Awards Best Education Project (2023) – for the Enhancing Cyber Security Across the Australian University Sector project.
- *The Australian* Research Awards (2023) – CCSRI ranked #2 Cyber Security Research Institute in Australia.
- RMIT University Vice-Chancellor's Award for Research Excellence – Team Award (2023) – for the Gender Dimensions in the Australian Security Industry project.
- RMIT University College of Business and Law Awards – COBL Award for Research Partnership and Impact (2022) – for the Enhancing Cyber Security Across the Australian University Sector project team.
- AISA Best Researcher of the Year Award (2020) – Professor Matt Warren, Cyber Researcher of the Year.

"Cyber security continues to be one of the top areas for investment in Australia's strategic research priorities."

4 CCSRI Research Themes and Domains

Research Themes

One of the distinguishing features of the RMIT Centre for Cyber Security Research and Innovation is its location within the RMIT University College of Business and Law, with an emphasis beyond technology, and a focus on the organisational and human elements of cyber security. This brings a truly multi-disciplinary approach to the way the Centre conducts impactful research and innovation and achieves research and education outcomes.



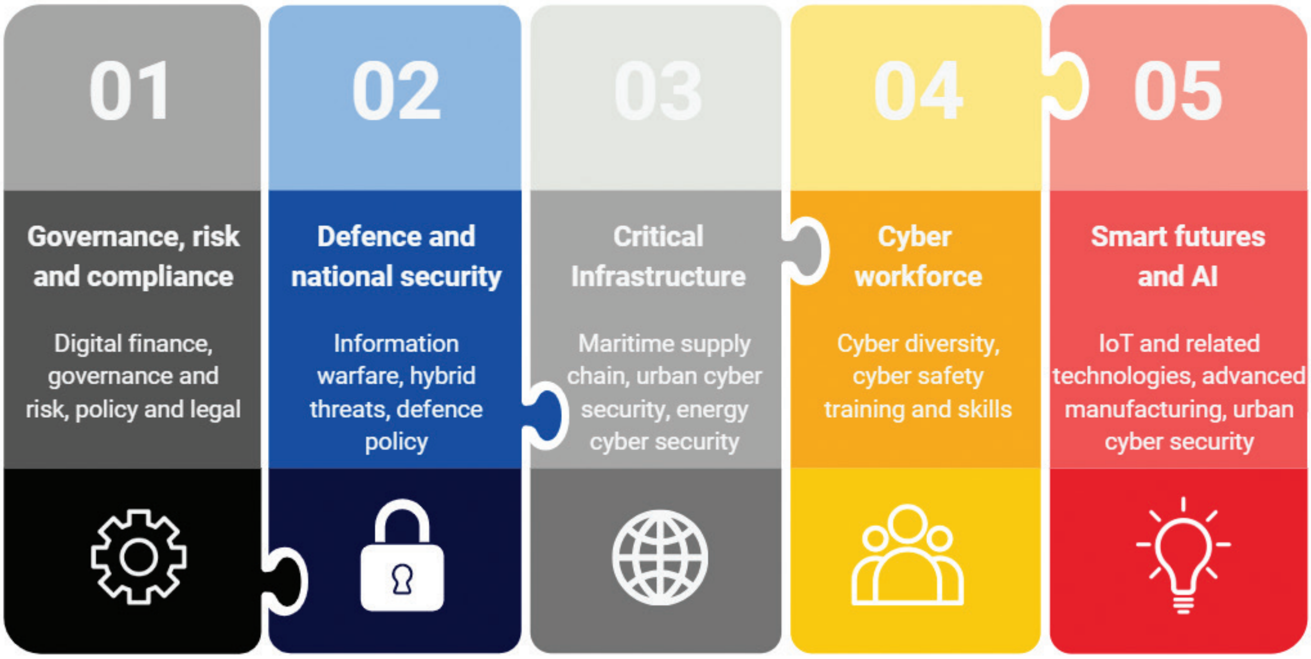
Human-centred

Technological

Organisational

Domain Capability

Engaging in a wide range of projects, our academic expertise, strong links to research partners, and consideration of technological and social dimensions, drive CCSRI to find solutions to critical problems impacting communities and the environment. The Centre's capability in these areas spans the following domains.



01

Governance, risk and compliance

Digital finance, governance and risk, policy and legal

02

Defence and national security

Information warfare, hybrid threats, defence policy

03

Critical Infrastructure

Maritime supply chain, urban cyber security, energy cyber security

04

Cyber workforce

Cyber diversity, cyber safety training and skills

05

Smart futures and AI

IoT and related technologies, advanced manufacturing, urban cyber security

5 Industry Advisors and Partnerships

The RMIT Centre for Cyber Security Research and Innovation collaborates closely and strategically with industry, government, and research agencies to enhance Australia's national cyber security capability and facilitate meaningful impact both in Australia and internationally.

RMIT Cyber Industry Advisory Board

The Centre draws upon a dynamic group of business and technology executives and cyber professionals to inform the multitude of educational and research programs in this field. Representing major companies and organisations from around Australia, board members contribute first-hand knowledge and diverse executive perspectives regarding key industry priorities and challenges. This knowledge enables continuous refinement of RMIT strategic direction relating to cyber security research and innovation.

The Centre's industry advisory board members have been instrumental in shaping the focus of research themes, as well as validating and collaborating on different cyber security education, research and uplift initiatives.

Collaborations and Partnerships

The Centre since its inception has collaborated closely with industry bodies, government agencies at both state and federal levels, international research groups, as well as industry organisations, on research projects and cyber security uplift initiatives.

Some of our most enduring partnerships, spanning multiple projects and iterations, include:

novatti

awsn
Australian Women in Security Network

AISA

Australian Government

Australian Government
Department of Foreign Affairs and Trade

Australian Government
Defence

Army

VICTORIA
State Government

International Presence

Beyond Australia, CCSRI has developed strong ties to the Asia-Pacific and European regions.

The CCSRI Vietnam Hub allows the Centre to strategically connect with and draw expertise from Vietnam and its neighbours. Critical to our impact in the region has been the close collaboration with the RMIT Vietnam team and the Vietnam Information Security Association (VNISA).

RMIT
UNIVERSITY
VIETNAM

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

RMIT University's European research campus has allowed us to make meaningful cyber security partnerships and contributions, particularly in the Baltic region in light of the geopolitical environment. Our strong connections with the Australian Lithuanian Cyber Research Network, through working partnerships with Mykolas Romeris University, has allowed for shared learnings and joint project collaborations.

MRU Mykolas Romeris University

AUSTRALIAN LITHUANIAN
CYBER RESEARCH NETWORK

6 Meaningful Impact

Industry and academic collaboration are at the core of all that we do at the RMIT Centre for Cyber Security Research and Innovation.

Working with organisations in a range of industries, our partnerships and projects deliver real-life practical solutions, along with strategic and policy related outcomes – from innovative research to impactful education and training programs.

The Centre prides itself on efficiently managing projects with internal and external stakeholders to deliver effective real-world outcomes.

On the following pages we share just some of the research and projects undertaken by the Centre that meaningfully contribute to:

- Addressing the cyber skills gap
- Securing critical infrastructure
- Strengthening Australia's defence and national security
- Forging international collaboration, and
- Exploring new boundaries.

Addressing the Cyber Skills Gap

Creating a More Inclusive Cyber Security Workforce for Women in Australia

Cyber security is integral to the effective operation and security of Australian institutions, government bodies, businesses and private citizens. Despite rapid sector growth in response to industry skill shortages, the cyber security workforce has a significant gender disparity, with women significantly under-represented in the sector. In 2023, groundbreaking research by the CCSRI revealed that women made up only 17% of cyber security professionals in Australia and that this lack of gender diversity in the cyber security sector results in an industry that is not performing to its full potential. Such significant gender disparity reduces the effectiveness of Australia's cyber security workforce and warrants further research in the area.

The detailed report released in early 2023 examined the gender dimensions of the Australian cyber security industry. A multi-disciplinary collaboration between the CCSRI, the Australian Women in Security Network (AWSN), and the RMIT Centre for Organisation and Social Change (COSC), the report painted a picture of an industry characterised by significant gender disparity, a lack of female mentors, and rapid attrition rates of women in the sector. The report was well-received by industry and made a marked impact in the cyber security space, finally putting concrete numbers behind the lived experience of many women in the industry. From these findings, the report made multiple recommendations to try to address gender diversity issues in the industry.

After the initial findings of the Phase I study revealed that most women leave the cyber security industry after just four years, CCSRI launched Phase II of the research aimed at gathering data on the explicit reasons why women left the industry in such high numbers. The Phase II study involved conducting in-depth interviews and investigating the barriers female cyber professionals encountered in their workplaces. As a result of this research, CCSRI and AWSN launched a joint policy paper aimed at industry and organisations to stem the high attrition rates of women in the cyber workforce.

The policy paper made specific, practical, and actionable recommendations, steering away from quotas and highlighting the need for flexible working hours and improved workplace culture.

Project Snapshot

Project
Gender Dimensions in the Australian Security Industry (Phases 1 and 2)

Collaboration
Australian Women in Security Network, RMIT Centre for Organisation and Social Change.

Key Contributors
Prof Matthew Warren, Dr Leonora Risse, Dr Maria Beamond, Dr Joanne Hall, Assoc Prof Lena Wang, Dr Banya Barua, Laki Kondylas.

Area of Focus
Improving gender equity in the Australian cyber security industry.

Outcomes
Detailed analysis of barriers and enablers for women working in the Australian cyber security industry, recommendations for improving the representation of women in the sector, and a policy paper focusing on practical strategies to improve gender equity in the sector.

> **"[The report's] recommendations can help put us on the path to achieving gender equity in the sector – without which, we won't be able to achieve our true cyber security potential."**
>
> *Hon. Clare O'Neil, former Minister for Home Affairs and Minister for Cyber Security*

Digital Skills and Cyber Security: Securing Our Future

In 2020, the COVID19 pandemic ground societies and workplaces to a halt across the globe. Employees and employers alike needed to navigate new ways of digital collaboration while remaining at home. Experts believe the pandemic fast tracked the role of technology in the workplace, in public life, and in people's personal lives, making it an integral part of life in a connected city.

The Victorian Higher Education State Investment Fund (VHESIF) commissioned a research initiative known as the Digital CBD Project. This research initiative included a series of five reports and a final roadmap to provide direction on how cities could become Digital CBDs with Melbourne positioned as a pilot city to lead the way.

As part of this project, in 2022, CCSRI set out to examine the shortfall in digital skills within the Victorian workforce revealed by the COVID19 pandemic and to illuminate a roadmap for Melbourne to become an effective and successful 'Digital CBD' by addressing these skill gaps. The report produced by RMIT was Part 4 of a five-part series, creating a comprehensive plan to bring together government, industry, education and individuals to ensure Melbourne remains a world leader in liveability and innovation.

The Future of the Digital CBD: Melbourne and Beyond report was created in collaboration with the RMIT Blockchain Innovation Hub and sought to create actionable recommendations within the context of COVID19's impact on working arrangements and the current level of digital skills within Melbourne. As part of the in-depth research, CCSRI conducted a survey to determine the effect COVID19 had on individuals working throughout the pandemic and their outlook on digital skills in the workplace. Critically, the majority of respondents believed that the two most pressing challenges in keeping the workforce secure were the lack of security awareness among remote workforces and keeping up with the latest cyber security threats.

Working from home exposes workers to more cyber threats, with much higher levels of digital interaction required, increasing the chance of security breaches. The report also found that as a result of COVID19, many organisations felt less cyber secure and that there was also a significant shortfall in the number of professionals with appropriate cyber security skills.

While COVID19 was a highly disruptive event, it exposed rather than caused the gaps in Melbourne's efforts to become a highly sophisticated Digital CBD. The CCSRI report presented practical recommendations to help elevate the digital skill level of Melbourne's workforces, increase the diversity of the workforce, and safeguard the future of digital skills. These recommendations included:

- The creation of a Victorian Digital Skills Academy
- Establishing a Cyber Security Accreditation Body and an Australian Cyber Security Body of Knowledge
- Enacting an ICT and Cyber Security Diversity Action Plan for Victoria
- Increasing skilled migration to aid Victoria's recovery
- Investing in innovative school programs that highlight the skills required in a digital economy
- Creating a program to increase the awareness of digital technologies and the need to upskill digital skills within the Melbourne CBD.

Together these recommendations work to address the ICT and cyber security skills gap to ensure Melbourne can fulfil its potential as a leading Digital CBD.

54% felt COVID-19 had left the organisation more exposed to cyber security threats.

25% felt they had adequate cyber security staff.

70% note a skills shortage in the workplace.

Project Snapshot

Project
The Future of the Digital CBD – Vic Skills Report

Collaboration
RMIT Blockchain Innovation Hub, RMIT Digital Ethnography Research Centre.

Key Contributors
Dr Ahmad Salehi Shahraki, Dr Konrad Peszynski, Dr Banya Barua, Laki Kondylas, Amarens Breteler.

Area of Focus
In-depth research and actionable recommendations to elevate the digital skill level of Melbourne's workforces, increase the diversity of the workforce, and safeguard the future of digital skills.

Outcomes
Practical recommendations to address the ICT and cyber security skills gap to ensure Melbourne can fulfil its potential as a leading Digital CBD.

Designing Safer and More Secure Digital Systems, Products and Services

In a digital world where cyber attacks, data breaches, and online threats are increasing both in number and sophistication, developing online products, services and systems that have safety, security and privacy at their core has never been more critical.

To assist developers and organisations to build online products and services with safety and security at their core, CCSRI developed two self-paced on-demand short courses – Safety by Design and Security by Design – and made them available free of charge on the e-learning platform, FutureLearn. These courses are designed for anyone interested in understanding how to embed Safety by Design and Security by Design principles and practices into the design, development and delivery of online products and services.

Safety by Design

When designing online products and services, it is important to invest in risk mitigation at the front end and embed user protections from the beginning. Knowledge of user safety is crucial to help up-and-coming tech leaders prevent their platforms and services being unintentionally weaponised to carry out abuse.

Jointly developed by Australia's eSafety Commissioner and CCSRI, the Safety by Design short course equips learners with the tools and skills to design online products and services with online safety and user rights at the core. Using the principles of Safety by Design, learners gain essential knowledge to minimise online threats by anticipating, detecting, and eliminating online harms before they occur.

The interactive course examines the basics of user safety, introduces Safety by Design principles and practices, and gives learners the opportunity to use eSafety's Safety by Design industry assessment tools. To date over 650 people from 83 countries have completed one or more components of the Safety by Design course.

Security by Design

The Security by Design short course developed by CCSRI gives learners the tools and knowledge to design, develop, and release online products and services with security at their core. Learners explore Security by Design principles and practices and learn why security is an important aspect of online product and service design, development and deployment.

The interactive course examines the key principles of Security by Design, explores how these principles can be applied to the Internet of Things, and provides an opportunity to consider the application of Security by Design principles and practices to real-life case studies.

The objective of these two short courses is to:

- Position Safety by Design and Security by Design at the centre of the design and development processes for online products and services.
- Identify the ways technology companies can minimise online threats through the design and development of online products and services by anticipating, detecting and eliminating user safety and cyber security threats before they occur.
- Implement practices which help to embed online safety and security into the culture and leadership of the organisation.
- Apply the principles of Safety by Design and Security by Design to the design, development and deployment of online products and services.

To date over 675 people from 90 countries have completed one or more components of the Security by Design course.

Project Snapshot

Project
Safety by Design and Security by Design Short Courses

Collaboration
eSafety Commissioner.

Key Contributors
Prof Matthew Warren, Dr Abebe Diro, Lee-ann Phillips.

Area of Focus
Equipping developers and organisations with the skills and knowledge to design, develop and deploy online products and services with user safety and cyber security embedded within.

Outcomes
Safety by Design and Security by Design self-paced on-demand short courses for those interested in developing and implementing online products and services with user safety and security at their core.

Helping Business Professionals Transition into Cyber Security Roles

With funding from the Australian Government Department of Education Microcredential Pilot in Higher Education initiative, CCSRI developed the Cyber Security Foundations for Business Professionals microcredential. The online foundational skills-based 12-week learning program is designed for business professionals from adjacent sectors and workforces seeking to develop skills in cyber security governance and risk management to support transition to governance and risk management roles in the cyber security sector.

Co-designed with industry and RMIT academics, the microcredential provides knowledge and skills related to cyber security governance frameworks, risk management strategies, and cyber security best practices to manage and mitigate cyber security risks.

As part of the microcredential, learners were given the opportunity to:

- Analyse and evaluate fundamental cyber security concepts and cyber security governance principles
- Construct cyber security artefacts such as security strategies and risk management frameworks
- Utilising a cyber security strategy and policy, develop an integrated and comprehensive cyber security program, and
- Analyse and appraise the legal, ethical and privacy considerations in relation to cyber security governance and emerging technologies.

Upon successful completion of the microcredential, learners were awarded a digital credential and were eligible for credit transfer for postgraduate business Masters programs at RMIT University.

Project Snapshot

Project

Cyber Security Foundations for Business Professionals Microcredential

Collaboration

RMIT Cyber Industry Advisory Board members, and the RMIT School of Accounting, Information Systems and Supply Chain. This project was supported with funding from the Australian Government Department of Education's Microcredential Pilot in Higher Education initiative.

Key Contributors

RMIT project team lead by Prof Matt Warren.

Area of Focus

Cyber security governance and risk management education for business professionals designed to assist those from adjacent industry sectors and workforces transition to cyber security governance and risk management roles.

Outcomes

A 12-week learning program for business professionals focusing on cyber security governance and risk management frameworks, processes and practices, that provides a digital credential and credit transfer into RMIT business postgraduate programs.

Co-Designing Inclusive Cyber Security Curricula for Higher Education

In today's cyber threat landscape, human vulnerabilities remain one of the most exploited entry points, particularly through phishing and social engineering. These risks disproportionately affect women, gender-diverse individuals, and culturally and linguistically diverse (CALD) communities due to barriers such as language, access to education, and social isolation.

Despite this, cyber security curricula in Australian higher education largely remains one-dimensional—focusing heavily on technical skills while neglecting the diverse, lived experiences of students. This gap in education hinders both student engagement and the broader development of an inclusive cyber security workforce.

The Co-Designing Inclusive Cyber Security Curricula in Australian Higher Education project aims to address this critical issue by reimagining cyber security education through the lens of intersectionality—considering how overlapping identities such as gender, culture, and socioeconomic background influence students' experiences and vulnerabilities in cyberspace.

By re-centering the voices of underrepresented groups in curriculum design, this work aims to boost engagement and retention in cyber security programs while also strengthening Australia's cyber resilience through a more diverse talent pipeline.

Project Snapshot

Project

Co-Designing Inclusive Cyber Security Curricula in Australian Higher Education: Integrating Intersectionality for Enhanced Student Engagement

Collaboration

RMIT University, University of Adelaide, University of Tasmania. Project funded by the Australasian Council of Deans of ICT (ACDICT), Australia.

Key Contributors

RMIT University: Assoc Prof Nalin Arachchilage (Lead Investigator), Dr Asangi Jayatilaka, Dr Senuri Wijenayake, Dr Gabrielle Murray, Prof Gary Thomas, Pro Vice-Chancellor, Indigenous Education.

University of Adelaide: Assoc Prof Claudia Szabo.

University of Tasmania: Assoc Prof Nicole Herbert, Dr David Herbert.

Area of Focus

The project prioritises inclusive education, cultural understanding, and social equity in cyber security, focusing on the human dimension of cyber threats and how organisational change in higher education curricula can address them.

Outcomes

- Mapped and critically reviewed current cyber security modules across multiple Australian universities to identify inclusivity gaps.
- Initiated a national series of co-design workshops involving 60+ students from diverse backgrounds to collaboratively reimagine more culturally inclusive curricula.
- Engaged academic staff, learning designers, and industry experts to co-develop practical guidelines for integrating intersectional perspectives into cyber security education.
- Dissemination of findings through a knowledge sharing workshop, comprehensive report, and a Q1-ranked journal publication.
- Contributed to the revamp of RMIT's Master of Cyber Security program with a culturally responsive framework.

> **"Cyber security is not just a technical issue—it's deeply human. By embedding intersectionality into cyber security education, we're not just closing skill gaps, we're empowering underrepresented communities to become resilient defenders in the digital age. This project is about transforming education to reflect the lived realities of students and building a more inclusive, secure future for all."**
>
> *Assoc Prof Nalin Arachchilage, School of Computing Technologies, RMIT University*

Securing Our Critical Infrastructure

Enhancing Cyber Security Across the Australian University Sector

Higher education institutions have emerged as a high priority target for cyber attacks. To safeguard Australia's higher education institutions, the Australian government established the Enhancing Cyber Security Across Australia's University Sector project in order to research the cyber security capability and resilience of the Australian university sector.

CCSRI was engaged to investigate the existing cyber resilience capacity of Australia's higher education system and to develop pathways to improve this capacity and further safeguard universities. The research undertaken by the Enhancing Cyber Security Across Australia's University Sector Project was the first of its kind, in how it approached improving cyber security across the entire Australian university sector. This research aimed to measure preparedness of Australia's universities for any potential cyber threat, while also identifying ways of improving the security of the sector's research, data, and personnel against cyber security breaches and foreign interference.

Throughout the project, CCSRI critically examined the sector's pre-existing mechanisms to receive and share threat intelligence, aided in connecting the sector to existing threat sharing mechanism platforms, developed an online tool to help create further threat models and mechanisms, and developed a suite of over 40 resources in line with government resources to assist universities with upskilling their communities. University representatives who utilised the resources have described the content as being extremely comprehensive and of exceptional quality.

In a testament to the breadth and quality of this research, CCSRI won the 2023 iTnews Benchmark Award for the Best Educational Project for its impactful work on enhancing cyber security across Australia's university sector. As of 2024, through the Tertiary Education Quality and Standards Agency (TEQSA), the resources developed for the program have been expanded to the entire higher education sector within Australia.

Additionally, through six Trusted Cyber Security Forums hosted by CCSRI, a trusted and nationally recognised peak forum for senior university members who have accountabilities relating to cyber security was established. The forums were extremely successful, with over 500 attendees from all 39 Australian public universities in attendance and over 30 different government, university and industry speakers presented on cyber security topics.

The impact of this research project is ongoing as it continues to uplift the cyber resilience of the higher education sector in Australia. With all resources made available to those education institutions that wish to access them, the project continues to contribute to a more secure cyber ecosystem defined by established norms and best practices.

Project Snapshot

Project
Enhancing Cyber Security Across the Australian University Sector

Collaboration
Department of Education, Department of Home Affairs, Australian Cyber Security Centre.

Key Contributors
RMIT project team lead by Prof Matt Warren.

Area of Focus
Enhancing and uplifting the cyber security of Australian universities.

Outcomes

- Connecting the Australian university sector to existing threat intelligence and threat sharing mechanisms and development of an online tool to help create further threat models and mechanisms.
- Development of 40+ resources to assist universities with upskilling their communities.
- Establishment of Trusted Cyber Security Forums for senior university members with accountabilities relating to cyber security.

Improving the Uptake of International Standards in the Australian Mining Industry

In recent years a growing number of cyber breaches among mining and utility companies has been reported, indicating a rising interest of malicious actors in the mining and minerals sector as an attractive target. As governments and business become increasingly aware of the importance of cyber security within critical infrastructure sectors, concern grows over the ability of the mining sector to resist cyber attacks. In this context, CCSRI was approached by the Joint Accreditation System of Australia and New Zealand (JAS-ANZ) to examine the adoption and effectiveness of three international standards—ISO/IEC 27001 (Information Security), ISO 55001 (Asset Management), and ISO 22301 (Business Continuity Management)—in the Australian minerals and mining industry.

Research conducted by CSSRI found that the implementation of these standards was particularly low, with many organisations simply opting to follow the NIST Cybersecurity Framework or the Australian Essential Eight. This low level of implementation of the ISO standards was due to several compounding factors, such as the high cost of implementation, perceived complexity and a low prioritisation of cyber security expertise, especially by small and medium sized enterprises (SMEs) in the sector. Even among larger organisations, implementation and certification of ISO standards was extremely low.

Over the course of the project, CCSRI held workshops and interviews with industry members and experts. During the interview phase, experts expressed that the wider mining industry continued to significantly underestimate the importance of cyber security standards. Current industry practices enable the use of many outdated software systems, insufficient cyber security training of non-IT staff members, and a lack of industry-wide norms to ensure a standard level of cyber resilience in the sector. Experts also reported that ISO standards were often perceived as too resource intensive, time-consuming and too complicated, leading to continued low implementation rates.

While there are barriers to ISO standard implementation, CCSRI strongly recommended the Australian mining and minerals industry adopt these standards, particularly ISO/IEC 27001 (Information Security) and ISO 22301 (Business Continuity Management) as the benefits of greatly improved cyber resilience and stakeholder confidence are key for critical infrastructure sectors.

CCSRI's project report recommended multiple practical actions targeted to different stakeholder groups, including government, industry bodies, and mining and minerals companies. These recommendations focused on making the implementation of ISO standards more affordable for companies, urged government to create industry requirements for cyber security training within the mining sector, and encouraged mining companies to educate their executives on the importance of cyber resilience.

This in-depth report commissioned by JAS-ANZ represents RMIT's spirit of industry engagement, calling for a comprehensive and holistic approach to improving overall cyber maturity of the Australian minerals and mining industry. Through greater industry implementation of ISO standards, the industry can insulate itself against the growing number of cyber attacks, ensuring greatly improved cyber resilience in a key critical infrastructure sector for Australian prosperity.

Project Snapshot

Project

Cyber Security and Asset Management in the Australian Mining and Minerals Sector

Collaboration

Joint Accreditation System of Australia and New Zealand (JAS-ANZ).

Key Contributors

Dr Arezoo Ghazanfari, Dr Banya Barua, Dr Konrad Peszynski, Dr Abebe Diro, Prof Matthew Warren, Laki Kondylas.

Area of Focus

Analysis of the implementation of three ISO standards in the Australian minerals and mining industry and factors impeding implementation as well as strategies to improve uptake of the standards.

Outcomes

Practical strategies to improve the implementation of three international standards —ISO/IEC 27001 (Information Security), ISO 55001 (Asset Management), and ISO 22301 (Business Continuity Management)— in the Australian minerals and mining industry.

Addressing Australia's Space Cyber Security Challenges

In 2024, researchers from CCSRI undertook an investigation into Australia's preparedness to respond to space cyber security vulnerabilities and identify opportunities to enhance its resilience. Sponsored by the Australian Government Department of Defence as part of their Strategic Policy Grants Program, the researchers sought to systematically address the complexity of space cyber security, encompassing its three vital dimensions: human, technological, and regulatory frameworks in the Australian context. Encompassing a multi-disciplinary team, the project engaged stakeholders belonging to industry, academia, defence, and government. In a series of workshops and interviews with the space and cyber sector, researchers engaged key stakeholders in workshops and interviews across Australia.

Adopting a phased research agenda, the research team:

- Conducted a threat assessment drawing on the current literature to identify cyber security attack vectors in space.
- Reviewed the existing counterstrategies and mitigation techniques used to tackle cyber threats related to space, and to evaluate Australia's space defence capabilities.
- Took a future perspective approach to cyber threat vectors, examining vulnerabilities to Australia's space sector.

Employing a scenario mapping methodology, researchers set out to examine current space cyber security Key Performance Indicators; space spectrum policy; the economic impacts of space cyber attacks; norms of behaviour in space; liability of space cyber attacks; and, changing power dynamics in the space commercialisation era.

A major outcome of the project was a report, inclusive of an impact analysis of security and resilience of Australian space activities, and a policy analysis, with recommendations for the defence sector and the Australian Government to enhance the safeguarding of Australian space assets.

Project Snapshot

Project
Australia Space Cyber Security Challenges, Anticipated Readiness, and Future Directions

Collaboration
Wise Law. This project is funded by the Department of Defence through a strategic policy grant.

Key Contributors
Prof Matt Warren, Dr Shah Khalid Khan, Dr Abebe Diro, Dr Adam Bartley, Amal Varghese, Georgina Power.

Area of Focus
Examination of Australia's space cyber security environment to analyse challenges, anticipated readiness, and future directions.

Outcomes
Analysis of Australia's space cyber security and development a comprehensive framework that integrates space and cyber domains, and development of innovative techniques for threat assessment and scenario mapping.

Strengthening Australia's Defence and National Security

Minimising the Threat of Autonomous Uncrewed Underwater Vehicles

Uncrewed underwater vehicles (UUVs) have recently emerged as major disruptive force in modern maritime warfare. UUVs pose a threat to undersea infrastructure, including cable infrastructure and shipping lanes. This capability, enhanced with future AI technologies, presents a relatively low-cost option for malicious actors. This issue isn't just a concern for the distant future; the 2022 Nord Stream pipeline sabotage and damage suffered by the Baltic Connector pipeline has highlighted the effectiveness of undersea infrastructure warfare tactics. This is a significant concern for a nation like Australia which relies on sea transport for 99% of its exports.

Funded through the Strategic Policy Grants Program from the Australian Department of Defence, this project embodies the collaborative nature of CCSRI, as this research was conducted alongside Charles Darwin University, and Wise Law to analyse and examine the modern landscape of UUVs in an Australian context. The project report and its recommendations represent an exhaustive analysis examining UUV development, vulnerabilities in Australian critical maritime infrastructure, and risk management practices. To generate these insights, consultations and workshops were undertaken with over 50 stakeholders from members of government public service, the Department of Defence, the Royal Australian Navy (RAN), defence industry, and researchers.

Australia is not adequately prepared for the possibility of future UUV use. Our current naval defences are not designed to deal with UUV deployment or AI smart mines, instead emphasising manned nuclear submarine development. The unmanned nature of UUVs allows them to be deployed extremely covertly, with the potential to cause massive damage to the undersea infrastructure on which Australia relies. Globally, there are multiple key shipping lanes which would be highly disruptive targets for UUV sabotage, including the Suez Canal and the Malacca Strait. While UUVs are likely to be state-owned initially, the possibility of non-state actors acquiring them in the future is a distinct and highly concerning possibility.

Within the report, CCSRI, Charles Darwin University, and Wise Law provide highly detailed and targeted recommendations for the consideration of both the Australian Government and Department of Defence. These recommendations included clarifying legal parameters for UUV deployment, incorporating the role of UUV operations and AI-enabled infrastructure in maritime security strategy, as well as enhancing surveillance and monitoring capabilities.

The project report emphasises that the timeframe for Australia to adequately respond to the new dimension UUVs bring to the modern defence landscape is rapidly closing, due to the speed of innovation in this space. CCSRI strongly recommends that indicators of government planning and response to the challenges posed by UUVs should be re-assessed regularly to ensure adequate progress is being made to safeguard Australia now and into the future.

Project Snapshot

Project

Australia's Trade and the Threat of Autonomous Uncrewed Underwater Vehicles

Collaboration

RMIT CCSRI, Charles Darwin University and Wise Law were collaborative research partners on this project, which was supported with funding from the Department of Defence's Strategic Policy Grants Program.

Key Contributors

Special thanks to our research partners: EJ Wise, Charles Darwin University staff involved – Prof Hamish Campbell, Prof Mamoun Alazab and Victor Abramowicz, and RMIT University staff involved – Prof Nirajan Shiwakoti, Dr Peter Stasinopoulos, Prof Asha Rao, Prof Ibrahim Khalil, Meredith Jones, Dr Shah Khalid Khan, Dr Adam Bartley, Prof Aiden Warren, Prof Matthew Warren, and Laki Kondylas.

Area of Focus

Analysis of UUV development, vulnerabilities in Australian critical maritime infrastructure, and risk management practices.

Outcomes

Targeted recommendations for the Australian Government to clarify the legal parameters for UUV deployment, incorporate the role of UUV operations and AI-enabled infrastructure in maritime security strategy, and the enhancement of surveillance and monitoring capabilities.

Establishing a Tri-lateral AI Security Dialogue Between Australia, USA and Japan

In recent years Artificial Intelligence (AI) has emerged as a key driver of economic growth and technological innovation, a trend likely to continue into the future. Against the backdrop of increasing global tensions, fragmentation of economic trade and supply chains, and intensified technological competition, the global reliance on AI technologies is deepening, and pooling resources and expertise has become essential to harness the full potential of AI-driven innovations.

To navigate this 'new normal', countries such as Australia, Japan, and the USA are increasingly aligned in terms of strategy and policy to assess the implications of widespread AI usage and associated next-generation technologies. Supported by the Australian Department of Defence, CCSRI, alongside researchers from the Pacific Forum, compiled a high-level assessment of potential strategic policy responses toward AI-enabled capabilities of Australia, Japan and the USA. The Tri-lateral Security Dialogue (TSD) is a strategic framework of state security cooperation between these three nations and serves to facilitate a robust, dynamic and productive dialogue.

Utilising this unique dialogue pathway to explore practical policy responses for the TSD on AI, the CCSRI and Pacific Forum developed an AI capability framework comprising four foundational elements:

Innovation *Advancing AI research and development.*

Ethics *Adoption of AI principles and standards to ensure responsible, reliable and human-centric AI deployment.*

Interoperability *Highlights the importance of joint military exercises and knowledge sharing to enhance operational resilience.*

Security *Implementation of security-by-design principles to safeguard AI-enabled technologies against cyber-enabled threats and ensure data privacy.*

Through strategic connections like the TSD, the three countries can capitalise on their joint capabilities to address the elements of this AI capability framework. This will enable members to respond quickly to emerging AI security challenges, help advance regional stability, and assist members in maintaining their status as global technology leaders.

The AI capability framework advanced in the paper is a highly useful policy tool for security policymakers, and industry practitioners. It serves as a flexible lens to understand the disruptive impacts of AI in the evolving threat landscape in the Indo-Pacific region from the perspective of the USA and Japan. Given the rapid AI development and innovation heralded by new breakthroughs like large language models, the AI capability framework affords policymakers a future-proof tool to navigate the ever-changing technology environment by not losing sight of the fundamental elements that underpin AI such as ethics, interoperability, and security.

Project Snapshot

Project
Australia's AI Strategy – Collaboration Across USA, Japan and Australia

Collaboration
Pacific Forum. This project was funded by the Australian Department of Defence.

Key Contributors
Prof Aiden Warren, Prof Charles T. Hunt, Prof Matthew Warren, Dr Adam Bartley, Mark Bryan Manantan.

Area of Focus
A high-level assessment of potential strategic policy responses toward AI-enabled capabilities of Australia, the USA and Japan.

Outcomes
Establishment of the Tri-lateral Security Dialogue (TSD), a strategic framework of state security cooperation security between Australia, Japan and the USA designed to facilitate dialogue and strategy on AI-enabled capabilities, and development of an AI capability framework.

Building a Security-Resilience Framework for Maritime Supply Chains in the Indo-Pacific

By volume, about 99% of Australia's trade is carried by sea mainly through the Indo-Pacific region. Global shipping trade valued around USD3.37 trillion is passed through the South China Sea, where Strait of Malacca is one of the busiest oil/energy shipping routes in the world. The region is subject to increasing maritime security threats due to territorial disputes and the risk of military conflicts. This project examines emerging security challenges facing maritime supply chains in the Indo-Pacific region and the implications for Australia, and it comprises four component studies.

1 Analysis of maritime security threats in the South China Sea and the broader Indo-Pacific

The first study is a scenario analysis of maritime security threats in the South China Sea and the broader Indo-Pacific that are associated with three contexts: South China Sea conflict, cyber attack on Australian maritime information systems, and Indo-Pacific maritime logistics network disruption.

The result of this analysis indicates that South China Sea conflicts would cause shipping capacity shortage, port operations breakdown, production disruption, technology failures, international armed conflicts, trade sanctions/embargo and diversion. These will likely result in an economic downturn, critical supplies, maritime supply chain disruptions, and increasing military activities in the region.

Cyber attacks on Australian maritime information systems will cause navigation operations disruption, cyber operations disruption, social technical disruption, human resource issues, and maritime supply chain disruption. These in turn have further impacts on Australia including port congestion and disruption of commercial shipping and supply chain operations.

Disruption of the Indo-Pacific maritime logistics network can be caused by factors other than those mentioned above. These can be competitive responses/interaction between countries or large organisations; disruptive innovation; geopolitical disruptions; ecological disruptions; and, trade related disruptions. These could have impacts on Australia including disruption of IT systems and trade networks, port and shipping operations, supply chain operations, critical supply shortages, loss of human lives, exhaustion of emergency rescue and security capabilities, economic downturn and social unrest.

2 Analysis of the vulnerability of tanker shipping network

The second study analysed the vulnerability of the tanker shipping network that Australia relies on for fuel supplies using Auto Identification System data. The analysis result indicates that while Australia's energy trade with Malaysia, Indonesia, Singapore, the US, Japan, Taiwan (China), Vietnam and the Philippines is not critically exposed to maritime security threats in South China Sea and East China Sea, energy trade of the latter countries is substantially exposed to tanker operations disruption caused by a closure of the South China Sea and East China Sea. As a result, Australia may join allies and other countries in the region in ensuring the Freedom of Navigation Operations (FONOPS) and upholding the rules-based international maritime order.

3 Analysis of the impact of cyber attacks on Australian maritime information systems

The third study highlighted the vulnerabilities of the Australian maritime industry due to cyber attacks and analyses the potential impact of cyber attacks on Australian maritime information systems under five cyber security threat scenarios, namely attacks on Australian destined shipping in the Malacca Straits; attacks on Australian bound shipping in the Lombok Strait; attacks on Australian bound shipping due to ransomware cyber breaches; maritime supply chain disruption due to data breach; and, maritime supply chain disruption due to cyber blockade. The third study also provides a number of recommendations for the improvement of cyber security.

4 Proposal for a national security-resilience framework for maritime supply chains

The fourth study proposed a national security-resilience framework for maritime supply chains, recapitulates security threats and advances strategies to enhance preparation and prevention, recovery from and adaptation to supply chain disruptions in the Indo-Pacific region. A focus group workshop was held to identify national security risks, resource and capacity constraints, and draw policy implications and recommendations for national resilience strategies. Several security issues and constraints facing Australia's maritime supply chains were identified as a result of the workshop.

As a result of these four studies, strategic policy recommendations were made to address the identified security risks and constraints. This includes Australia taking a more active role in the region through international relations and cooperation, focusing not only on warfare and defence elements but also shifting trade patterns and building alliances with friendly countries in the region.

> **"The character of warfare is changing, with more options for pursuing strategic ends just below the threshold of traditional armed conflict – what some experts like to call grey-zone tactics or hybrid warfare."**
>
> *Senator Linda Reynolds, former Minister for Defence (2019)*

Project Snapshot

Project

Maritime Supply Chain Security in the Indo-Pacific Region

Collaboration

Australian Maritime College, Curtin University, University of Tasmania.

Key Contributors

Assoc Prof Hong-Oanh Nguyen, Michael Van Balen, Aaron Ingram, Stephen Hurd, Prof Prem Chhetri, Prof Vinh Thai, Prof Matthew Warren, Prof Booi Kam, Assoc Prof Richard Oloruntoba.

Area of Focus

Examination of emerging security challenges facing maritime supply chains in the Indo-Pacific region and the implications for Australia, including threats and policy implications for national security and resilience.

Outcomes

Analysis of security challenges facing maritime supply chains in the Indo-Pacific region and a proposal for a national security-resilience framework for maritime supply chains.

Lessons Learned from Information Warfare in the Ukraine-Russia Conflict

The war in Ukraine (from 2020 to the present) has expertly utilised a key tool in modern conflicts, that being information in the form of Information Warfare (IW), which operates across strategic, operational, and tactical levels, blending civilian and military efforts. Russia's persistent use of cyber attacks, disinformation, and propaganda, as well as the exertion of influence, have been major drivers in efforts to disrupt Ukraine's political and military operations. In response to Russia's use of IW, Ukraine has taken advantage of IW with a concerted focus on using open source intelligence, strategic communications, and counter-disinformation to combat Russia's IW strategy. As a result of Ukraine's own IW efforts, and challenging Russia's IW, Ukraine has shown remarkable resilience and use of IW to secure substantial international support.

In the Baltic nations (Estonia, Latvia, and Lithuania) the Ukraine conflict has highlighted the potential for conflict spillover, and the geographic range of information operations and their impact on regional societal architectures. This leads to the question: How does Australia prepare for its own IW challenge? The unique circumstances of the Russia-Ukraine war and clear understanding of who the aggressor is and how they should be countered indicate that any translatable lessons must be critically evaluated and contextualised. This brings critical focus to questions as to what constitutes an act of war in the information space, and how the Australian Army deals with that problem.

With funding from the Australian Army Research Centre and the Department of Defence, CCSRI conducted research into potential IW challenges for Australia. The research team from RMIT University adopted a multi-faceted approach to gather a comprehensive body of empirical data, conducting workshops and interviews across Lithuania, Latvia, and Estonia. This provided access to diverse perspectives on IW, allowing for a nuanced analysis of the challenges faced by Ukraine.

The research involved a wide range of stakeholders, including active military personnel from multiple countries, former military advisers, NATO representatives, government professionals, academics, think tank experts, civilians, and members of volunteer national army units. The various backgrounds of the participants enabled the study to capture a nuanced and versatile dataset, with unique insights from strategic, operational, and grassroots level perspectives.

The research also involved a literature review and analysis, which examined non-academic reports, policy briefs, white papers, and operational documents from governments, NATO, non-government organisations, and think tanks. Acknowledging the increasing role played by digital platforms in modern hybrid warfare, the research included an analysis of social media activity on the Telegram and X (formerly Twitter) platforms that have been used as key communication tools by both Ukrainian and Russian actors, as well as established information sharing networks within and beyond the conflict.

The report produced as a result of this research project conveys, in a wartime-conflict scenario, the lessons of Ukraine for Australia, emphasising the need for dynamic information operations, agile structures of control, flexible processes of civil military engagement, and strategic communications activation across all levels of the Army.

Additionally, the report highlights that systemic civil military engagement must extend beyond the traditional domains of defence to include partnerships with civil society organisations, academic institutions, private industry, and technology platforms. For Australia, these lessons highlight the imperative to cultivate a whole of society approach to IW, ensuring that military and civilian partners work together to protect against this complex situation.

Project Snapshot

Project
Ukraine: Information Warfare

Collaboration
CCSRI thanks the Australian Army Research Centre and the Department of Defence for sponsoring this project.

Sincere thanks for the support provided by our partners and affiliates in Estonia, Lithuania and Latvia, especially the NATO Cooperative Cyber Defence Centre of Excellence, Estonia, NATO's Strategic Communications Centre of Excellence, Latvia, and Mykolas Romeris University, Lithuania.

Key Contributors
Prof Matthew Warren, Dr Adam Bartley and Prof Aiden Warren with contributions from Dr Malka Halgamuge, Valerii Paziuk, Tom Saxton, Meredith Jones, Amal Varghese, Laki Kondylas, and Lee-ann Phillips.

Area of Focus
Research and analysis of the use of Information Warfare in the Russia-Ukraine conflict and the learnings for Australia in the context of conflict involving conventional and information warfare.

Outcomes
Report analysing the use of Information Warfare in the Russia-Ukraine conflict and the considerations and challenges that the Australian Army faces in the context of conflict involving conventional and information warfare.

Effective Cyber Security Partnerships – Lessons from Ukraine

The war in Ukraine (2020 - present) has demonstrated the importance of government partnerships with private organisations. The Ukrainian experience has highlighted that security is core to digital transformation, and public-private cyber partnerships have been an important element in Ukraine in terms of Western IT companies providing cyber tools, services and intelligence, as well as volunteer cyber groups set up to support Ukraine. The Ukrainian government has been successful in developing these key partnerships because they have been based on a trusted relationship over an extended period of time.

The research project has taken the RMIT team and its members to Estonia, Latvia and Lithuania and to the borders of Russia and Belarus to understand the complexity of the partnership between defence, society and private companies in the Ukrainian context.

This project employed a qualitative research design structured in three phases designed to examine the role and effectiveness of cyber partnerships in Ukraine. The research integrates multiple sources of data, including open-source intelligence, literature review, expert interviews, and policy analysis, to develop a comprehensive understanding of cyber security defence collaborations.

Research analysis indicates that Australia can learn from the Ukrainian experience in terms of the need to develop a strong Australian public-private cyber partnership model, methods of working with international organisations, development of an Australian Cyber Reserve, and the ways in which we can build stronger relationships with our European partners.

The Ukrainian experience has highlighted the importance of national agility and being able to adapt security relationships and partnerships and react to different situations as they evolve. This will help Australia to anticipate future trends and challenges in order to stay ahead of its adversaries. Simultaneously Australia also needs to further develop its own sovereign capability, especially in the cyber security domain.

The project report provided insights drawn from the Russia-Ukraine conflict and included key recommendations on how Defence and the Australian Army could potentially work with civil society and industry to bolster Australia's cyber capacity and anticipate, withstand, recover from, and adapt to the everchanging cyber threat landscape.

Project Snapshot

Project

Ukraine: Cyber Security – Partnership Between Defence, Society and Private Companies – Lessons from Ukraine

Collaboration

CCSRI thanks the Australian Army Research Centre and the Department of Defence for sponsoring this project.

Sincere thanks for the support provided by our partners and affiliates in Estonia, Lithuania and Latvia, especially the NATO Cooperative Cyber Defence Centre of Excellence, Estonia, NATO's Strategic Communications Centre of Excellence, Latvia, and Mykolas Romeris University, Lithuania.

Key Contributors

Prof Matt Warren, Prof Aiden Warren, Dr Adam Bartley, with contributions from Dr Malka N. Halgamuge, Valerii Paziuk, Tom Saxton, Meredith Jones, Laki Kondylas, Amal Varghese and Lee-ann Phillips.

Area of Focus

Examination of the role and effectiveness of cyber partnerships in Ukraine to develop a comprehensive understanding of cyber security defence collaborations and how the lessons from Ukraine can help Australia build better public-private-civil partnerships to enhance cyber security.

Outcomes

Report drawing on the experiences of Russia-Ukraine conflict and key partnerships with civil society and private companies, with recommendations on how the Australian Government can work with civil society and industry to bolster Australia's cyber capacity and build resilience to the evolving cyber threat landscape.

Forging International Collaboration

Enhancing Cyber Security Awareness and Capacity Building for Vietnamese SMEs

As the digital landscape continues to evolve, cyber security has become a crucial aspect of economic growth and prosperity for countries worldwide.

Vietnam's rapidly expanding digital ecosystem offers numerous opportunities and at the same time exposes organisations to a myriad of cyber threats. Small and medium-sized enterprises (SMEs) in Vietnam encounter various challenges that concern cyber security. However, this highlights the ongoing and potential collaborative efforts between Australia and Vietnam in addressing these cyber security challenges.

The Australia Vietnam Policy Institute (AVPI) together with the RMIT University Centre for Cyber Security Research and Innovation released a policy briefing outlining the current cyber security landscape in Vietnam, and ways of enhancing cyber security awareness and developing cyber resilience. Supported by the Australian Department of Foreign Affairs and Trade, this policy brief offers recommendations and insights for improving these enterprises' cyber security awareness and capacity building.

Key takeaways from this policy briefing include:

- Increasing cyber security across South East Asia is crucial for the region's future economic growth, security and stability of our shared region.
- Focusing on enhancing cyber resilience for SMEs in Vietnam is vital to ensure the sustainability and development of the nation's digital economy and strengthen the Australia-Vietnam relationship.
- Tailored cyber security solutions and training programs should be developed and it is beneficial to partner with government and industry associations to organise workshops, train-the-trainer programs, and resource portals.
- By fostering international partnerships, we can bring together stakeholders and resources worldwide to enhance cyber security awareness and capacity building for Vietnamese SMEs.
- A comprehensive approach that raises awareness, builds capacity, and fosters collaboration among stakeholders is essential.

Project Snapshot

Project
AVPI Policy Briefing: Enhancing Cyber Security Awareness and Capacity Building for SMEs in Vietnam

Collaboration
RMIT CCSRI, RMIT University Vietnam, Department of Foreign Affairs and Trade, Australia Vietnam Policy Institute (AVPI).

Area of Focus
Analysis of the current cyber security landscape in Vietnam, and ways of enhancing cyber security awareness and developing cyber resilience of SMEs.

Outcomes
Policy paper with recommendations and insights for improving the cyber security awareness and capacity building of Vietnamese SMEs.

Delivering Cyber Security Uplift in Vietnam

In 2023, with funding from the Department of Foreign Affairs and Trade (DFAT), CCSRI designed and delivered significant cyber security training and support to Vietnamese SMEs and larger corporate entities under the Cyber and Critical Technology Cooperation Program (CCTCP) Cyber Ambassador and Corporate Bootcamp programs. These programs raised awareness of cyber security issues and practices while building capacity within Vietnam. CCSRI's method focused on 'training the trainer' in specific organisations, helping to ensure future knowledge sharing within Vietnam's SME cyber security community.

Working collaboratively with the Vietnam Information Security Association (VNISA) and RMIT Vietnam, CCSRI built significant relationships within the Vietnamese business community, as the training materials were delivered in Vietnam and in the native language. The program impact reached beyond the SME space, with training eventually delivered to larger industry entities such as Vietnam Airlines and Vietcombank. CCSRI has trained over 1,300 Vietnamese professionals, including over 400 Vietnamese women.

In addition to the initial SME program success, CCSRI identified that Vietnam's critical infrastructure providers also desired cyber resilience training. Building on the foundation laid, CCSRI expanded the project with a second phase that focused on delivering Vietnam-specific cyber security training to enhance the cyber resilience, preparedness and response of Vietnamese critical infrastructure providers (e.g. telecommunications, finance, ports, utilities, airlines etc). The program was successfully delivered to over 800 cyber professionals working in critical infrastructure in Vietnam.

Project Snapshot

Project

Cyber and Critical Technology Cooperation Program (CCTCP) in Vietnam

Collaboration

Vietnam Information Security Association (VNISA), RMIT Vietnam.

Key Contributors

RMIT Melbourne CCSRI team: Prof Matt Warren, Laki Kondylas, Amal Varghese, Gabriela Cincotta, Lee-ann Phillips, Violet Leonard.

RMIT Vietnam team: Assoc Prof Hiep Cong Pham (Director, CCSRI Vietnam Hub), Dr Duy Dang, Tu Anh La, Bony Pham, Kim-Ngan Cao, Trang Bui, Linh Nguyen (Hazel).

Industry experts: EJ Wise, Richard Magalad, John O'Driscoll, Chathura Abeydeera.

Academic trainers: Dr Akanksha Saini, Dr Amy Corman, Dr Arathi Arakala, Duy Dang, Dr Geetika Verma, Dr Mahshid Sedaghapour, Assoc Prof Nalin Arachchilage, Dr Shah Khalid Khan.

Area of Focus

Design and delivery of cyber security training and support to Vietnamese SMEs and larger corporate entities under the CCTCP Cyber Ambassador and Corporate Bootcamp programs to uplift cyber security in Vietnam.

Outcomes

Cyber security uplift program delivery to 1300+ Vietnamese professionals, including 271 cyber professionals employed in critical infrastructure services.

Empowering Emerging Women Cyber Security Leaders in Vietnam

An exciting addition to the Cyber and Critical Technology Cooperation Project (CCTCP) in 2025 was the development and delivery of a women's cyber security leadership program for emerging female leaders in Vietnam, the She Leads Digital: Emerging Female Leaders in Cyber Security program. The program focused on leadership, digital maturity, and cyber security for mid-career women in the cyber and digital transformation sectors.

The She Leads Digital initiative provided targeted support, mentorship, and leadership opportunities for female cyber professionals in Vietnam, striving to close the gender gap and empower women in technology in the South East Asia. The two-day program, delivered to over 50 female emerging cyber leaders, covered both leadership and cyber security topics, such as, leadership in the technology sector, emerging cyber trends, creating a cyber-safe culture, and understanding the legal and policy dimensions of digital transformation.

The successful delivery of this CCTCP cyber capacity-building program embodied CCSRI's mission to create a more gender inclusive cyber security industry in the Asia-Pacific region.

Project Snapshot

Project
Cyber and Critical Technology Cooperation Program (CCTCP) – She Leads Digital: Emerging Female Leaders in Cyber Security

Collaboration
RMIT Vietnam, Vietnam Information Security Association, Department of Foreign Affairs and Trade.

Key Contributors
RMIT Melbourne CCSRI team: Prof Matt Warren, Laki Kondylas, Amal Varghese, Gabriela Cincotta, Violet Leonard.

RMIT Vietnam team: Assoc Prof Hiep Cong Pham (Director, CCSRI Vietnam Hub), Duy Dang, Bony Pham, Kim-Ngan Cao, Trang Bui, Linh Nguyen (Hazel).

Industry experts/academic trainers: EJ Wise, Dr Geetika Verma.

Area of Focus
Design and delivery of cyber security awareness and capability training to emerging female cyber security leaders in Vietnam.

Outcomes
Delivery of a two-day cyber security uplift program for women in cyber leadership to 50+ female emerging cyber leaders in Vietnam.

Building Cyber Awareness and Capability in Cambodia

With significant cyber security program foundations laid in Vietnam to uplift cyber awareness and capabilities, in 2025 CCSRI expanded the program into Cambodia as part of the Cyber and Critical Technology Cooperation Program (CCTCP).

In 2025 CCSRI delivered its Cyber Ambassador and Cyber Bootcamp training programs in Cambodia, focussing on building cyber resilience in the critical infrastructure services, as part of DFAT's South East Asia and Pacific Cyber Program (SEA-PAC Cyber) program.

The training programs were designed to identify and uplift the cyber awareness and capability of critical infrastructure providers, and increase understanding of the importance of cyber incident preparedness, as well as increase regional interest and engagement in cyber security and safety. The Cambodian CCTCP training was successfully delivered to over 200 professionals and government personnel employed in critical infrastructure services and helped to facilitate a network of connected cyber professionals in Cambodia.

The CCTCP cyber capacity-building program embodies CCSRI's mission to forge a lasting impact and provide real-world solutions through an integrative approach to cyber security, positioning the Centre as a leading source of research, education and innovation both in Australia and internationally.

Project Snapshot

Project
Cyber and Critical Technology Cooperation Program (CCTCP) in Cambodia

Collaboration
RMIT Vietnam, Ministry of Post and Telecommunications, Cambodia, Department of Foreign Affairs South East Asia and Pacific Cyber Program (SEA-PAC Cyber).

Key Contributors
RMIT CCSRI team: Prof Matt Warren, Laki Kondylas, Amal Varghese, Gabriela Cincotta, Violet Leonard.

RMIT Vietnam: Assoc Prof Hiep Cong Pham (Director, CCSRI Vietnam Hub), Bony Pham, Kim-Ngan Cao, Trang Bui, Linh Nguyen (Hazel), Prof Robert McClelland.

Industry experts: EJ Wise, Richard Magalad, John O'Driscoll, Chathura Abeydeera.

Academic trainers: Dr Arathi Arakala, Dr Mahshid Sedaghapour.

Area of Focus
Design and delivery of cyber security awareness and capability uplift training through the CCSRI Cyber Ambassador and Corporate Bootcamp programs to Cambodian professionals working in critical infrastructure.

Outcomes
Cyber security awareness and capability uplift program delivered to 200+ cyber professionals and government personnel working in critical infrastructure services in Cambodia.

Improving Digital Readiness and Resilience in ASEAN Education Institutions

Australia seeks to improve the digital readiness and resilience of Technical and Vocational Education and Training (TVET) systems in ASEAN (Association of South East Asian Nations). To meet this goal for improved cyber security collaboration and regional uplift in the TVET sector, CCSRI has successfully delivered five short courses on ‘Improving the Digital Readiness and Resilience of TVET Systems in ASEAN’ funded through the DFAT Australian Awards program. Each participant is an industry professional and received an Australian Awards Fellowship to attend the course.

This short course, hosted in Australia, enabled participants to visit Melbourne and Adelaide, showcasing both Australian culture and Australia’s commitment to building meaningful regional collaboration in the cyber uplift space. Over the two-week program, participants engaged with a range of learning delivery formats, including presentations, workshops, site visits, networking events and conferences. The content focused on the importance the digital readiness and building the resilience of the delegate’s various institutions, while also covering secure online training delivery.

This diverse range of delivery methods and carefully selected experts involved in program design and delivery sets CCSRI up for success in our cyber uplift programs.

To date, CCSRI has run five iterations of the course, in partnership with Vector Consulting, training more than 120 leading professionals in the technical and vocational education training sectors in their home countries. The participants have hailed from nine ASEAN member states, creating networking opportunities to connect professionals across the region.

The success of this course is a key example of the practical way CCSRI is committed to contributing to the global cyber security innovation ecosystem. By facilitating professional learning opportunities such as this, CCSRI uplifts the talents of Australia’s ASEAN partners, making the region a safer and more collaborative environment.

Project Snapshot

Project
Improving the Digital Readiness and Resilience of TVET Systems in ASEAN

Collaboration
DFAT Australia Awards Program. Project funded by the Department of Foreign Affairs and Trade.

Key Contributors
RMIT CCSRI, Australian Cyber Collaboration Centre, Vector Consulting.

Area of Focus
Development and delivery of a two-week intensive program for TVET (Technical and Vocational Education and Training) professionals from South East Asian nations with the aim to improve the digital readiness and resilience of TVET systems in ASEAN and to improve cyber security collaboration and regional uplift in the TVET sector.

Outcomes
To date, the TVET course has been delivered five times, training more than 120 leading TVET sector professionals from nine ASEAN member states, creating networking opportunities to connect professionals across the region.

Enhancing Cyber Security Across the University Sector in the Pacific

As regional cooperation becomes increasingly relevant in cyber maturity, CCSRI has been privileged to host multiple Australia Award Fellowship programs on behalf of the Department of Foreign Affairs and Trade. Australia strongly believes in contributing to the cyber uplift of its regional neighbours to facilitate a safe and secure Pacific. To further this regional knowledge sharing, in 2024 CCSRI welcomed 15 Australia Award Fellowship delegates from Fiji University and the University of the South Pacific (Cook Islands, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Samoa, Solomon Islands, Tokelau, Tonga, Tuvalu, and Vanuatu) to participate in the Enhancing Cyber Security Across the University Sector in the Pacific program.

The program began with three days at the Australian Information Security Association's CyberCon 2024 convention, providing delegates with the opportunity to shape their own learning experiences, choosing from hundreds of informative sessions and tailoring their programs to suit their own organisational and personal needs.

Following AISA CyberCon 2024, the program continued with a productive first week of workshops and learning opportunities that focused on the Australian cyber security landscape, emerging technologies and AI, as well as examination of the national cyber security strategy and best practices to protect critical infrastructure such as higher education institutions.

In the second week, the delegates experienced a digital transformation case study and workshop, with practical insights into the digital evolution to take back to their own higher education institutions. Sessions focused on online safety for diverse groups, the impact of data privacy considerations for both Australia and the South Pacific, as well as the importance of a strong cyber culture. The participants were also presented with examples of cyber strategy and business contingency planning, highlighting the importance of preparedness and strategic foresight in maintaining cyber resilience.

Over the course of the program, the participants had the opportunity to engage with presenters from multiple government departments, industry bodies and major organisations, providing access to an array of perspectives and highly experienced experts, creating a valuable learning experience.

Alongside CCSRI's practical role as a research and cyber education organisation, we aim to create lasting connections between our overseas participants, Australia and RMIT University itself.

> **"The way RMIT structured this training has put technicalities at the forefront and allowed ample time for processing and digesting content, differentiating itself from other training providers. It has been extremely successful structuring it this way. I will go home and aim to practice all the learnings."**
>
> *Program participant*

Project Snapshot

Project

Enhancing Cyber Security Across the University Sector in the Pacific

Collaboration

Fiji University and the University of the South Pacific.

Area of Focus

Development and delivery of a two-week intensive program for professionals from Fiji University and the University of the South Pacific with the aim to improve the digital readiness and resilience of higher education institutions in the South Pacific and to improve cyber security collaboration and regional uplift in the sector.

Outcomes

Delivery of a two-week intensive cyber security and resilience educational program for university sector professionals from Fiji.

Connecting the Australian and Lithuanian Cyber Security Sectors

The Australian Lithuanian Cyber Research Network (ALCRN) is a joint initiative between RMIT University and Mykolas Romeris University. The Network launched in February 2022, with the goal to connect cyber security researchers, students, and industry and government practitioners working on and/or interested in Australia and Lithuania.

The ALCRN aims to:

- Promote increased awareness and understanding of the state of cyber security and associated issues within the network, as well as more broadly within Australian and Lithuanian society.
- Support Australian and Lithuanian cyber activities by sharing knowledge, skills, expertise, experiences, plans, policies, procedures, and practices.
- Conduct joint research on identified cyber security trends, risks, threats, impacts, and controls as well as future disruptions. The cyber research relates to the organisational, human, technical and legal aspects of cyber security, including cyber threats and influence on a democratic society.

The first initiative of the ALCRN was the launch of the Australian-Lithuanian Hybrid Threat Centre. Hybrid threats are state and non-state actors that are challenging countries and institutions they see as a threat, opponent, or competitor to their interests and goals with a focus on disrupting industry and society. This is the first national Hybrid Threat Centre in Australia. The Australian–Lithuanian Hybrid Threat Centre:

- Undertakes joint research looking at hybrid threat impacts upon Australia and Lithuania
- Assesses the society and organisational impact of hybrid threats
- Explores the impact of hybrid threats upon countries critical infrastructure including democratic institutions
- Develops joint seminars exploring hybrid threat issues, and
- Writes thought leadership items regarding the impact of hybrid threats.

AUSTRALIAN LITHUANIAN
CYBER RESEARCH NETWORK

Project Snapshot

Project
Australian Lithuanian Cyber Research Network

Collaboration
Mykolas Romeris University.

Key Contributors
Australian Co-Director: Prof Matt Warren, (2022+).

Lithuanian Co-Director: Prof Marius Laurinaitis (2024+), Prof Darius Stitilis (2022-2024).

Area of Focus
Promoting awareness, understanding and research of the state of cyber security within Australian and Lithuanian society.

Outcomes
Joint research projects and seminars relating to hybrid threats, and thought leadership items on the impact of hybrid threats.

> **"Lithuania has been facing hybrid cyber threats for several years, mainly from the Russian side. Over the past few years, Lithuania has acquired some experience and seeks to share this experience with other countries, as well as to further research preventive measures and countermeasures against hybrid threats. The established centre is an example of such activity, as well as a great example of cooperation between Lithuania and Australia."**
>
> *Co-convenor of the ALCRN,*
> *Professor Darius Štitilis,*
> *Mykolas Romeris University*

Exploring New Boundaries

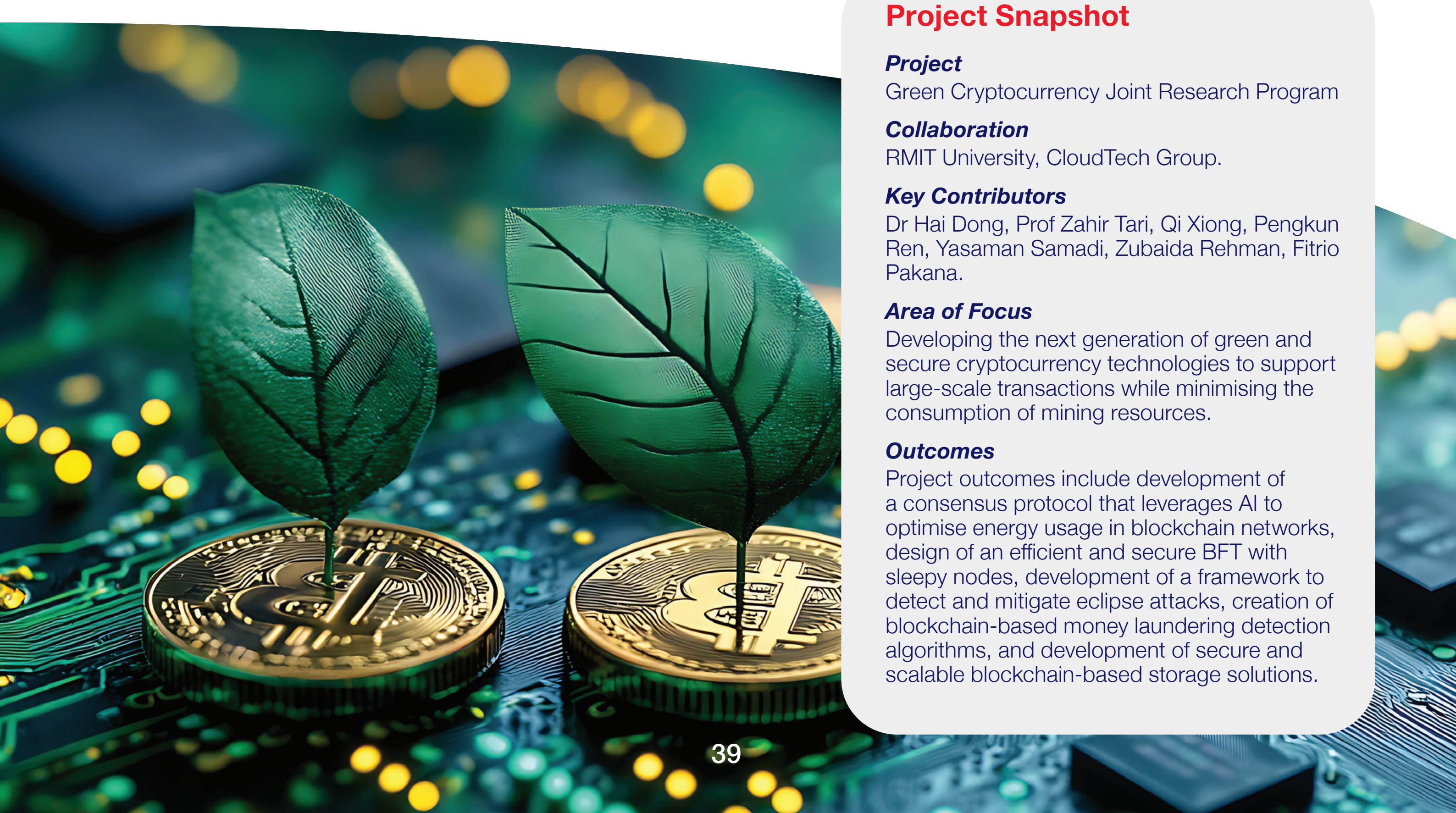
Advancing the Next Generation of Green and Secure Cryptocurrency Technologies

This project focuses on developing the next generation of green and secure cryptocurrency technologies to support large-scale transactions while minimising the consumption of mining resources and rationalising the use of storage resources to create value with the lowest input.

Project progress and achievements to date include:

- AI-Driven Energy-Efficient Consensus Protocol – development of a novel consensus mechanism that leverages artificial intelligence to optimise energy usage while maintaining fairness and decentralisation in blockchain networks.
- Efficient and Secure BFT with Sleepy Nodes – design of an efficient and secure Byzantine Fault Tolerant (BFT) model that supports 'sleepy' or intermittently active nodes, enabling efficiency without compromising consensus reliability.
- Eclipse Attack Prevention and Protection Frameworks – introduction of a robust framework to detect and mitigate eclipse attacks, enhancing the security and connectivity resilience of blockchain nodes in adversarial environments.
- Blockchain-Based Money Laundering Detection Algorithms – created intelligent detection algorithms capable of identifying suspicious transaction patterns and uncovering potential money laundering behaviours within blockchain systems.
- Resource-Efficient Blockchain Storage Frameworks – engineering of secure and scalable blockchain-based storage solutions that reduce redundancy and optimise storage utilisation for cost-effective data retention.

This joint research with CloudTech has laid a solid foundation for the future of sustainable blockchain technologies. By integrating AI into consensus algorithms, energy consumption has been significantly reduced while ensuring fairness. The work on sleepy BFT models and eclipse attack prevention frameworks enhances the security and resilience of blockchain networks. The project has also advanced the fight against financial crime with novel money laundering detection techniques and developed efficient blockchain-based storage systems. Collectively, these innovations represent a major leap toward a greener, safer, and more scalable cryptocurrency ecosystem.



Project Snapshot

Project
Green Cryptocurrency Joint Research Program

Collaboration
RMIT University, CloudTech Group.

Key Contributors
Dr Hai Dong, Prof Zahir Tari, Qi Xiong, Pengkun Ren, Yasaman Samadi, Zubaida Rehman, Fitrio Pakana.

Area of Focus
Developing the next generation of green and secure cryptocurrency technologies to support large-scale transactions while minimising the consumption of mining resources.

Outcomes
Project outcomes include development of a consensus protocol that leverages AI to optimise energy usage in blockchain networks, design of an efficient and secure BFT with sleepy nodes, development of a framework to detect and mitigate eclipse attacks, creation of blockchain-based money laundering detection algorithms, and development of secure and scalable blockchain-based storage solutions.

Fast and Secure Cryptocurrency Payments for e-Commerce Merchants

The global cryptocurrency market is an emerging means of exchange, valued at $3.12 trillion, with a 21% increment in daily transactions (2020-21). Despite the size and growth, diverse security and operational impediments pertinent to the currencies' liquidity and safety limit its usability.

Researchers, Zahir Tari, Nasrin Sohrabi, Md Redowan Mahmud, Matt Warren, Hai Dong and Qiang Fu, were successful in a joint bid for an Australian Government Cooperative Research Centres Project (CRC-P), receiving over $2.3 million in funding to address the diverse security and operational impediments pertinent to the crypto market with the goal to improve its usability.

As a result of this funding, in partnership with Novatti Group, thankQ Solutions Pty Ltd, and Swyftx, RMIT University through this project is developing a digital platform consisting of novel anti-fraud and anti-money laundering techniques, to align crypto transactions with traditional payment options such as credit cards. This will allow consumers, merchants, and exchanges to acquire, verify and transfer cryptocurrency with trust and scalability while conducting daily business. The project will modernise Australian industries to take the lead in leveraging such currencies globally.

Project Snapshot

Project
Fast and Secure Cryptocurrency Payments for e-Commerce Merchants

Collaboration
RMIT joint Cooperative Research Centre Project (CRC-P) with Novatti Group, thankQ Solutions Pty Ltd, Swyftx.

Key Contributors
Prof Zahir Tari, Dr Nasrin Prof Matt Warren, Prof Zahir Tari, Dr Hai Dong, Dr Qiang Fu (RMIT University), Dr Nasrin Sohrabi (Deakin University), Dr Md Redowan Mahmud (Curtin University).

Area of Focus
Address the diverse security and operational impediments pertinent to the cryptocurrency market with the goal to improve its usability.

Outcomes
Development of a digital platform consisting of novel anti-fraud and anti-money laundering techniques, to align cryptocurrency transactions with traditional payment options.

Investigating Cyber Security Challenges for Autonomous Vehicles

The adoption of Autonomous Vehicle Technology (AVT) poses a range of technical, behavioural, policy, and cyber security challenges.

This project aimed to develop a simulation tool that evaluates the direct and indirect impacts of Autonomous Vehicle (AV) deployment, incorporating factors such as technological maturity, consumer incentives, and data cyber security. The tool provides critical insights for stakeholders to assess 'what-if' policy and technology scenarios for effective deployment strategies for autonomous vehicles.

Project Snapshot

Project

Development of a Simulation Tool for Adoption and Deployment of Autonomous Vehicles

Collaboration

RMIT University School of Engineering, Forum 8 Pty Ltd (industry partner), Australian Government Department of Industry, Innovation and Science (Project ID: AEGP000050).

Key Contributors

Prof Nirajan Shiwakoti, Dr Peter Stasinopoulos, Prof Matthew Warren, Yilun Chen, Dr Shah Khalid Khan.

Area of Focus

Investigation of the technical, behavioural, policy, and cyber security challenges associated with Autonomous Vehicle Technology (AVT) and development of a simulation tool to capture the dynamics associated with the adoption of AVT.

Outcomes

- Development of one of the first comprehensive, theoretically grounded system dynamics-based simulation tools for AV deployment scenario analysis, including cyber risks.
- Pioneering survey-based study capturing four OECD countries, including Australia, to examine public perceptions of cyber risks and autonomous vehicles.
- Trained two PhD students and two masters (course based) students in AV systems and cyber security.
- Produced over 19 peer reviewed publications, including 15 high quality journal articles.

"This project laid the foundation for a new generation of tool and talent needed to guide Australia's transition to connected and autonomous vehicles. From consumer insights to cyber security readiness, our work bridges technical innovation with practical policy solutions."

Prof Nirajan Shiwakoti, RMIT University

Secure and Scalable Road Surface Monitoring

Australia's regional and remote roads face significant safety risks due to poor surface conditions, extreme weather, and limited inspection coverage. To address this, the Secure and Scalable Road Surface Monitoring via Fleet-Based Multi-Sensor Fusion project deploys vehicle-mounted sensing systems—such as cameras, GPS, and accelerometers—on existing fleet vehicles (e.g. garbage trucks, buses) to continuously monitor road surfaces in real-time.

In parallel, the project addresses critical cyber security challenges inherent in distributed sensing networks. When data is collected from multiple mobile sources across unsecured or partially trusted networks, it can be susceptible to deliberate interference, such as false data injection, replay attacks, or signal spoofing. The resilient filtering architecture is designed not only to improve data quality but also to serve as a first line of cyber defence by detecting and rejecting anomalous or malicious inputs before they can compromise the fused dataset. This capability ensures that road hazard detection decisions are based on verified, trustworthy information, safeguarding the system's integrity and maintaining reliable service continuity even under potential cyber attack scenarios.

> **"Our resilient filtering architecture provides the backbone for trusted sensor data fusion at scale – ensuring that even the most remote roads are monitored with the same reliability as urban networks."**
>
> *Dr Amirali Khodadadian Gostar, RMIT University*

Project Snapshot

Project

Secure and Scalable Road Surface Monitoring via Fleet-Based Multi-Sensor Fusion

Collaboration

RMIT University, National Road Safety Action Grants Program (NRSAGP), partner councils involved in pilot deployments (e.g. Shoalhaven, Noosa Shire), and industry collaborators in sensing and AI technologies.

Key Contributors

Dr Amirali Khodadadian Gostar, Prof Zahir Tari, Prof Alireza Bab-Hasdiashar.

Area of Focus

Secure sensor fusion, resilient data filtering, real-time hazard detection.

Outcomes

- Development of a cyber-resilient data fusion pipeline using a resilient filtering architecture to enable real-time monitoring of road hazards.
- Integration of cyber security mechanisms to detect and reject malicious or compromised measurements, protecting against false data injection, replay attacks, and sensor spoofing.
- Successful deployment of this architecture in pilot trials, supporting early detection and prioritisation of road surface defects.
- Demonstrated robust performance of the architecture in varied environments (urban to remote), even under challenging data quality conditions.

Protecting Data in Motion

Given the increasing amount of data being generated, as well as the daily incidences of data being breached, the need to protect this data while being generated and shared is growing. The impending arrival of quantum computers adds yet another dimension to this issue.

The concept of encrypting data at rest (when it is stored) and when it is shared is well researched and understood. However, the advent of IoT (Internet of Things), especially in the medical field has added further dimensions – these IoT devices are resource constrained and can rarely encrypt the data they collect. Furthermore, in the medical field, the vast amount of data collected by a variety of IoT devices needs to be analysed and fused together to enable clinicians to make informed decisions. Currently, data must be unencrypted to be analysed, which introduces a possible avenue for loss of privacy.

This project considers three aspects of data privacy:

1. Creation: How can data be secured when it is created (collected) by an IoT device?
2. Sharing: How can this data be shared in such a way that only the right person can access it?
3. Analysis: How can data be analysed while it is encrypted? How can different types of (medical) data be fused to provide a more holistic picture to the clinician?

> **"Mountains of data are being generated, especially in the medical realm. Being able to understand this data while still protecting the privacy of the individual is the current challenge facing the health sector – from researchers to clinicians, and the government. This project aims to address this important area keeping in mind the impending threat to privacy posed by quantum computing."**
>
> *Prof Asha Rao, RMIT University*

Project Snapshot

Project

Protecting Data in Motion: Encrypting Data During Computation

Collaboration

Information Security Research Group, School of Science, RMIT University; Commonwealth Scientific and Industrial Research Organisation (CSIRO); BITS-Pilani.

Key Contributors

Prof Asha Rao, Prof Neena Goveas, Dr Arathi Arakala, Dr Amy Corman, Dr Shubhangi Gawali, Dr James Baglin.

Area of Focus

Encrypting and protecting medical data during computation – collection, sharing and analysis – to ensure the privacy of individuals.

Outcomes

This project is ongoing and has resulted in several journal and conference articles, and one PhD completion to date. Another three PhD students are currently involved in different aspects of this research.

Developing Privacy-Preserving Collaborative Analytics Solutions on Sensitive Data

In many existing applications, large quantities of valuable and sensitive user data are collected. To realise mutual benefits, data owners may collaborate to combine data together from multiple sources and jointly perform analytical tasks over aggregated data. Such collaborative analytics is advantageous to enable more accurate medical studies, detection of financial crimes, more relevant online advertising. This is because data are intrinsically distributed. Combining data sources increases data volumes and diversity and provides much richer information for analysis.

Worryingly, current solutions for aggregating data typically operate on cleartext data without encryption. This raises severe privacy concerns, and poses hurdles to their practical adoption. Data are crowdsourced and often contain private or identifying information of individuals. These sensitive data should be always kept confidential and should not be shared across the boundaries of data sets. Furthermore, increasingly strict data privacy laws and regulations such as the *Privacy Act 1988* in Australia, HIPAA in USA, and GDPR in Europe forbid sensitive data being shared or pooled. In addition, organisations gather data from their own customers and invest to derive insights from such data. They deem the gathered data proprietary and are not willing to fully publish data due to business competition.

There is a pressing need to reimagine collaborative data analytics to function under conditions that ensure data privacy and protect business interests, while also providing the benefits of combining data sets.

This project aims to develop privacy-preserving collaborative analytics solutions on sensitive data. Such solutions promise to enable scenarios where multiple organisations can jointly execute data analytical tasks over their sensitive input data, without revealing any information beyond agreed upon results. The approach is to have each organisation adequately encrypt its sensitive data via advanced cryptographic privacy-enhancing techniques (i.e. secure multi-party computation techniques) before the data leaves its administrative trust domain. Then, a collaborative analytics system running across organisations proceeds with the encrypted data and generates an encrypted result that only can be decrypted by authorised parties.

Project Snapshot

Project

Privacy-Preserving Collaborative Analytics on Sensitive Data (LP220200649, 2023-2026)

Collaboration

Australian Research Council, RMIT School of Computing Technologies, Ansen Innovation.

Key Contributors

Prof Xun Yi, Prof Karin Verspoor, Dr Maggie Liu.

Area of Focus

Data privacy and security.

Outcomes

Project outcomes include a hybrid trust model with distributed trusts to provide malicious security guarantees, lightweight privacy-enhancing techniques to express rich analytical functionalities, and a system platform for real-world applications. This provides significant benefits such as facilitating industries to safeguard their customers' data and uplift their businesses in a secure and trustworthy fashion.

Enhancing Cyber Security Learning Through AI-Driven Gamification

As cyber threats become more complex and pervasive, the demand for skilled cyber security professionals continues to outpace supply. Traditional training methods often fail to engage learners or adapt to individual learning needs, particularly among diverse and non-technical user groups. With the rise of digital learning platforms, this project tackles a critical question: How can we use AI and gamification to make cyber security education engaging, inclusive, and effective?

The CyberAI project explores the development of a scalable, adaptive learning framework that leverages AI-driven support systems, serious games, and behavioural analysis to improve cyber security training.

In collaboration with OpenCyberAI and supported by RMIT, the research investigates how gamified platforms can personalise the learning experience, optimise user engagement, and improve long-term knowledge retention. It combines systematic benchmarking, user modelling, and data mining to create evidence-based, human-centred educational interventions that respond dynamically to real-world cyber security challenges.

> **"The future of cyber security education lies in understanding people—not just systems. By embedding AI into game-based learning, we're creating environments where users can safely explore threats, make mistakes, and learn in a way that's adaptive, inclusive, and grounded in real behavioural data."**
>
> *Assoc Prof Nalin Arachchilage, RMIT University*

Project Snapshot

Project

CyberAI: Enhancing Cyber Security Learning Through AI-Driven Gamification and Behavioural Insights

Collaboration

RMIT University (lead institution), OpenCyberAI, UK (technical partner and funding body).

Key Contributors

Assoc Prof Nalin Arachchilage (Chief Investigator, RMIT University), collaborators across OpenCyberAI, UK.

Area of Focus

This project bridges the gap between AI technology and human-centred design to improve cyber security knowledge and behaviour at scale. It combines organisational research into educational effectiveness with technical development and psychological insight.

Outcomes

- Development of a multi-phase methodology combining AI, gamification, and behavioural analytics to assess and enhance cyber security learning outcomes.
- Benchmarking of traditional and gamified training platforms, highlighting gaps and best practices across user types and demographics.
- Produced behavioural models of user interaction patterns, improving the design of adaptive learning paths.
- Designed serious game-based modules that simulate real-world cyber incidents (e.g. phishing, ransomware, network intrusion) with varying complexity.
- Collected empirical evidence showing increased engagement and knowledge retention in gamified environments over traditional approaches.
- Positioned to influence cyber security training in universities, professional upskilling, and policy development in human-centric cyber resilience.

Developing a Federated Fine-Tuning Framework for Secure and Collaborative GenAI Models

The rapid advancement of ChatGPT and related generative AI technologies, such as Large Language Models (LLMs) and Multimodal Foundation Models (MFMs), is significantly influencing various industry sectors. Foundation models are extensively trained machine learning models used as the basis for specialised tasks. MFMs, a subset of these, handle diverse data types like text, images, audio, and video. These technologies are being employed to analyse medical images, consolidate patient data, and revamp fields including energy, engineering, social services, and the creative industries. By enhancing data analysis, design optimisation, and content creation, they demonstrate a vast range of applications and the potential for quick adoption within Australian industries and the public sector.

Research by the Tech Council of Australia and Microsoft indicates generative AI could add up to $115 billion annually to Australia's economy in seven years, boosting growth by 2%-5%. However, challenges like limited computing power and the need for large datasets remain. Data privacy and security risks are major concerns, especially in healthcare, where reidentification of anonymised data is a threat. Recent breaches, such as those at Medibank and Optus, highlight potential financial and reputational risks.

The project aims to develop an advanced federated fine-tuning framework for GenAI models, capable of handling large-scale, heterogeneous datasets across multiple devices while ensuring strong data privacy and security. It also seeks to innovate resource-optimised quantisation strategies to deploy these models on resource-limited devices without sacrificing accuracy or performance. Additionally, the framework will integrate a variety of fine-tuning techniques to ensure computational efficiency and data privacy. Finally, it will develop defence mechanisms to counter adversarial threats and maintain data privacy, establishing a secure and trustworthy federated learning environment.

Project Snapshot

Project

Federated Fine-Tuning Framework for Secure and Collaborative GenAI Models (LP-240100417)

Collaboration

Australian Research Council, RMIT School of Computing Technologies, Serendib Systems.

Key Contributors

Prof Ibrahim Khalil, Prof Xun Yi.

Area of Focus

Exploration of the challenges of adoption of GenAI models across various sectors with the intent to establish a federated fine-tuning framework.

Outcomes

The framework focuses on fine-tuning LLMs and MFMs in secure, decentralised environments, improving their effectiveness. It includes the development of optimisation techniques for fine-tuning GenAI models on resource-limited devices and introduces new methodologies to tackle security and privacy challenges in federated fine-tuning.

> **"Generative AI is undoubtedly the future, but it carries with it inherent privacy and security challenges. To truly unlock its potential, we must confront and resolve these issues head-on."**
>
> *Ibrahim Khalil,*
> *PhD, Professor for Cloud Systems and Security,*
> *RMIT University*

7 Future Outlook

Over the past five years, the RMIT University Centre for Cyber Security Research and Innovation has been working closely with researchers across RMIT Australia and RMIT Vietnam, as well as working with various industry and government bodies, to produce key cyber security research and education projects with real-world impact.

So what does the next five years look like? What could some of the key future cyber security trends be? The future of cyber security will be shaped by the impact of new technologies such as quantum and accelerated post-quantum cryptography, secure AI deployment and applications, growing global cyber security skill shortages, more extensive cyber security regulations, and legal processes trying to catch up with the actual cyber security threats, as well as cyber security becoming more of a global challenge.

In this evolving landscape, cyber security is no longer just a technical issue, but rather there is growing awareness that it is equally a humanistic and organisational issue, and that it needs to be addressed with a considered and proactive multi-disciplinary approach. As cyber threats continue to grow in number, complexity and sophistication, and with the convergence of regulation, public awareness, and technological innovation playing a pivotal role in shaping cyber resilience, the Centre will continue to work closely with researchers, industry and government to build this cyber resilience both in Australia and on the international stage.

The RMIT Centre for Cyber Security Research and Innovation will continue to partner with researchers, industry and government to:

- Support industry, businesses and citizens to strengthen their cyber security and their defences against increasingly sophisticated cyber threats
- Strengthen cyber protections for critical infrastructure and uplift cyber security capability
- Grow and professionalise the cyber security workforce
- Shape and support a cyber resilient Asia-Pacific region.

Ultimately, the future of cyber security will be defined not just by the research undertaken, and tools that are built, but by how quickly we are able to adapt, collaborate, and anticipate cyber threats before they materialise.

Contact CCSRI

Website

Visit the CCSRI website at **https://rmit.edu.au/cyber**

Email

Contact us at **ccsri@rmit.edu.au**

Location

Building 80
445 Swanston Street, Melbourne, 3000
Victoria, Australia

Social Media

The Centre maintains an active presence on:

LinkedIn
https://www.linkedin.com/company/rmit-centre-for-cyber-security-research-and-innovation/

YouTube
https://www.youtube.com/@rmitcentrecybersecurityres9863

RMIT UNIVERSITY
Centre for Cyber Security Research and Innovation