Teaching the Future: Integrating Cybersecurity into Education

Faraz Khan

Victorian Skills Authority Fellowship, 2026

International Specialised Skills Institute

Victorian Skills Authority

First Published 2026

Report by Faraz Khan
Typeset by Danielle Cull
Printed by Elgin Printing

The International Specialised Skills Institute

1/189 Faraday St,
Carlton VIC 3053
info@issinstitute.org.au
+61 03 9347 4583

ISBN: 978-1-923561-15-1

Table of contents

01 Abbreviations, Acronyms And Key Definitions 1

02 Acknowledgements 2

03 Executive Summary of Fellowship 5

04 Fellowship Background 7

05 Fellowship Learnings and Findings 13

06 System-Level Issues, Recommendations and Next Steps 33

07 Impacs of Fellowship 41

08 Sector Engagement (Dissemination) 46

09 Conclusion 49

10 References 52

01

Abbreviations, Acronyms And Key Definitions

The following terms are used throughout this report. This list is intended to support readers who may be unfamiliar with cybersecurity, education or VET terminology.

Term	Meaning
ACS	Australian Computer Society
AISA	Australian Information Security Association
CISA	Cybersecurity and Infrastructure Security Agency (United States)
CSIRO	Commonwealth Scientific and Industrial Research Organisation
CTF	Capture the Flag: a practical cybersecurity challenge in which participants solve technical tasks in a safe environment
Cyber clinic	A supervised work-integrated learning model in which learners provide clearly defined cybersecurity support to eligible organisations
Cyber hygiene	Routine behaviours that reduce cyber risk, such as using strong authentication, applying updates and recognising phishing attempts
Cyber range	A safe, simulated environment used for practical cybersecurity learning, testing and exercises
Digital competence	The knowledge, skills and behaviours required to use digital technologies safely, effectively, critically and responsibly
EU CyberNet	A European Union-funded network supporting international cybersecurity capacity building
ISS Institute	International Specialised Skills Institute
K–12	School education from kindergarten to Year 12
NCyTE	National Cybersecurity Training and Education Center (United States)
NICE	National Initiative for Cybersecurity Education (United States)
NIST	National Institute of Standards and Technology (United States)
RIA	Estonian Information System Authority, which includes the National Cyber Security Centre of Estonia
RTO	Registered Training Organisation
VET	Vocational Education and Training
VSA	Victorian Skills Authority
VU	Victoria University
Work-integrated learning	Learning that incorporates authentic, supervised workplace experience or industry-based projects

02 Acknowledgements

The Awarding Bodies

The Fellow sincerely thanks the Victorian Skills Authority (VSA) for providing funding support for the ISS Institute and for this Fellowship.

The ISS Institute plays a pivotal role in creating value and opportunity, encouraging new thinking and early adoption of ideas and practice by investing in individuals. The overarching aim of the ISS Institute is to support the development of a 'Better Skilled Australia'. The Institute does this via the provision of Fellowships that allow Australians to undertake international skills development and applied research that will positively impact Australian industry and the broader community.

The ISS Institute was founded in 1991 by a small group of innovators, including Sir James Gobbo AC, CVO, QC, and former Governor of Victoria, who had a vision of building a community of industry specialists who would lead the up skilling of the Australian workforce.

The Fellowship program builds shared learning, leadership, and innovation across the broad range of industry sectors worked with. Fellows are supported to disseminate learning and ideas, facilitate change and advocate for best practices by sharing their Fellowship learnings with peers, colleagues, government, industry, and community. Since its establishment, ISS Institute has supported over 580 Fellows to undertake skill and knowledge enhancement across a wide range of sectors which has led to positive change, the adoption of best practice approaches and new ways of working in Australia.

The Fellowship programs are led by our partners and designed to achieve the needs and goals desired by the partners. ISS Institute works closely to develop a Fellowship program that meets key industry priorities, thus ensuring that the investment will have a lasting impact.

For further information on ISS Institute Fellows, refer to www.issinstitute.org.au

Governance and Management

- **Patron in Chief:** Lady Primrose Potter AC
- **Patrons:** Mr Tony Schiavello AO, Mr James MacKenzie and Mark Kerr
- **Founder:** Sir James Gobbo AC, CVO
- **Board Chair: Dr Bill Petreski**
- **Board Treasurer:** Adrian Capogreco CA
- **Board Secretary:** Alisia Romanin
- **Board Members:** Prof. Amalia Di Iorio AM, Robert Buckingham, Jeremy Gobbo KC and Susan Renouf
- **Chief Executive Officer:** Dr Katrina Jojkity

Sponsor - the Victorian Skills Authority

The Victorian Skills Authority works in partnership with the International Specialised Skills Institute by funding the VET International Practitioner Fellowships. The Fellowship program focuses on developing opportunities within the VET sector to assist in building an Education State in Victoria that produces excellence and reduces the impact of disadvantage. In addition, the program is funded to support the priorities of Skills First, including developing capacity and capability, innovative training practices and increasing teacher quality within the VET sector as well as building industry capability and developing Victoria's current and future workforce.

Fellow's Acknowledgements

It was a great honour to receive the VET International Practitioner Fellowship in April 2025. The Fellow is sincerely grateful to the International Specialised Skills Institute (ISS Institute) and the Victorian Skills Authority (VSA) for providing the opportunity to undertake this Fellowship and explore international approaches to cybersecurity education and workforce development.

The Fellow would like to acknowledge the guidance, encouragement, and support provided throughout the Fellowship journey by Dr Katrina Jojkity, Chief Executive Officer of the ISS Institute; Kay Schlesinger, Program Manager at the ISS Institute; and Anne-Maree Butt, former Senior Policy Officer at the Victorian Skills Authority. Their support and commitment to international knowledge exchange played a significant role in the successful completion of this Fellowship.

The Fellow would also like to express his deepest gratitude to his family for their unwavering support throughout the Fellowship. Completing this project required a significant commitment of time, including periods spent away from his young family. First and foremost, the Fellow would like to thank his wife, Yasmeen, whose encouragement, patience, and support made the completion of this Fellowship possible. The Fellow would also like to thank his children, Farya and Rayan. They continue to be great sources of strength, courage, and joy in his life and provided constant motivation throughout this journey.

The Fellow is grateful to Victoria University for providing the support and flexibility required to undertake and complete the Fellowship. Special thanks are extended to Janusz Dutka, Manager HE Diplomas, for his ongoing support throughout the Fellowship. The Fellow is also grateful to Dianne McKeagney, Director, Centre of VU Transitions, for her support and encouragement throughout the Fellowship. The Fellow would also like to acknowledge John Burgess, Manager, Cyber Security and Digital Technologies, who was the Fellow's manager at the time the Fellowship was awarded. The Fellow is also grateful to colleague Owen Smith, recipient of a 2024 ISS Institute Fellowship, who generously shared his experience and provided valuable mentorship throughout the Fellowship process.

The Fellow would like to acknowledge Rosemary Dore, former Education Product Development Manager at the Australian Computer Society (ACS), whose encouragement and support helped secure an important letter of support for the Fellowship application. The Fellow is also grateful to Siobhan O'Sullivan, Chief Operating Officer of the Australian Computer Society, and Megan Spielvogel, General Manager of the Australian Information Security Association (AISA), for their support and letters of endorsement.

The Fellow would like to thank Mona Sidhu from the New South Wales Department of Education and the members of the CyberMarvel Cyber Awareness Working Group for their ongoing collaboration and commitment to improving cybersecurity awareness and education across Australia. The Fellow also

thanks Elizabeth Paterson, Conference Producer and Event Operations Manager at EDUtech Australia, for providing opportunities to share Fellowship findings with the broader education community. The Fellow further acknowledges Patrick Kidd OBE OAM, Chief Executive Officer of the Future Skills Organisation, for providing the opportunity to connect with the Future Skills Organisation's ICT Training Package project.

The Fellow is deeply grateful to the many international experts, educators, researchers, and practitioners who generously shared their time, expertise, and insights throughout the Fellowship.

In the United States, special thanks are extended to Rodney J. Petersen, former Director of Education and Workforce for the Applied Cybersecurity Division at the National Institute of Standards and Technology (NIST); Dr Melissa Dark, founder of DARK Enterprises, Inc.; Dr Kristine Christensen, Program Director for the National Community College Cybersecurity Fellowship Program; Dr Keith E. Clement from Fresno State University and Chair of the Workforce Development and Education Subcommittee of the California Governor's Cybersecurity Taskforce; Michele Robinson, Senior Director and Principal Investigator of the National Cybersecurity Training and Education (NCyTE) Center; Dr Candi Ring of Operation K12; Shannon Beck, Director of the Virginia Cyber Range; Brandon Sally of Cyber.org; Stacy Sinclair of Fortinet; Kristi Rice, Chair of the Virginia Cyber Range K–12 Advisory Committee; Dr Davina Pruitt-Mentle, Lead for Academic Engagement in the National Initiative for Cybersecurity Education (NICE) Program at the National Institute of Standards and Technology (NIST), and Donna Woods, Head of Cyber AI Partnerships at Work Education California.

In Canada, the Fellow would like to thank Charles Finlay, founder of Rogers Cybersecure Catalyst, as well as Alysha St John and Jonathan Joynt from the Canadian Centre for Cyber Security for sharing their expertise and perspectives on cybersecurity workforce development, teacher education, and cyber awareness initiatives.

In Estonia, the Fellow would like to acknowledge Tiina Pau from the National Cyber Security Centre of Estonia (RIA); Elyna Heinmäe from Tallinn University; Meidi Sirk from Tallinn University; Lauri Aasmann and Liina Areng from EU CyberNet; Peadar Charles Callaghan from Tallinn University; and Dr Birgy Lorenz from Tallinn University of Technology. Their insights provided invaluable perspectives on digital competence, cybersecurity education, teacher capability development, and Estonia's internationally recognised approach to cyber resilience.

Finally, the Fellow would like to thank all the organisations, educators, policymakers, researchers, industry representatives, and stakeholders who contributed to this Fellowship. Their willingness to share experiences, challenges, and innovative practices has enriched this research and helped shape the findings and recommendations presented in this report.

03

Executive Summary of Fellowship

Cyber risk is no longer confined to ICT teams or specialist occupations. It is now embedded in every digitally enabled workplace, from health and community services to manufacturing, business, education and critical infrastructure. Yet Australia's education and training system does not consistently equip learners, educators or providers to respond. This Fellowship found that the central challenge is not a lack of activity, but a lack of connection: promising qualifications, resources, awareness programs and industry initiatives remain fragmented across policy, funding, curriculum, educator development and workforce pathways. For Victoria, this creates an urgent opportunity to position cybersecurity as a foundational workforce capability and strengthen the VET system's role in building a safer, more productive and future-ready economy.

Awarded in April 2025 and sponsored by the Victorian Skills Authority, the Fellowship, Teaching the Future: Integrating Cybersecurity into Education, examined how leading international systems integrate cybersecurity and digital safety into education, prepare teachers, create practical learning environments and connect learning with employment. The Fellow, Faraz Khan, is a vocational education teacher specialising in cybersecurity at Victoria University, where he has taught Certificate IV and Diploma of Cybersecurity programs since 2024. His experience showed that many learners enter specialist programs without a strong foundation in digital safety, responsible technology use or cybersecurity principles, while educators face limited time, confidence, resources and industry currency. These observations motivated the Fellowship and its focus on strengthening capability earlier and more consistently across the education pipeline.

The research combined Australian sector consultation, a survey of VET educators, policy and program review, participation in national and international conferences, site visits, interviews and continuing virtual engagement. From April 2025 through 2026, the Fellow engaged with education, government, industry and research leaders in the United States, Canada and Estonia. The United States was selected for its national workforce frameworks, educator development programs, cyber ranges and education-to-employment initiatives; Canada for its industry–education partnerships, workforce programs and cyber clinic model; and Estonia for its internationally recognised digital competence, cyber resilience and whole-of-system approach. Travel to the United States and Canada occurred in December 2025, while engagement with Estonia was undertaken virtually after the planned visit could not proceed.

Across the three countries, six interconnected lessons emerged. First, national frameworks and shared language provide direction without requiring a single uniform curriculum. Second, educator capability must be treated as essential workforce infrastructure, supported through funded professional learning, practical laboratories, mentoring, train-the-trainer models and industry externships. Third, learners need

equitable access to authentic practice through cyber ranges, simulations, competitions, gamified activities and supervised service-based learning. Fourth, cybersecurity should extend beyond ICT programs and be contextualised to the risks, responsibilities and technologies of different occupations. Fifth, strong workforce pipelines require clearer transitions between school, VET, higher education, certifications and employment, supported by recognition, mentoring, work-integrated learning and labour-market intelligence. Sixth, sustainable reform requires long-term funding, clear governance, institutional ownership, industry participation, and ongoing evaluation, rather than reliance on isolated or short-term initiatives.

The international evidence also showed what should be avoided: over-reliance on vendor-specific content, short-term grants without continuation plans, unequal access between well-resourced and smaller or regional providers, isolated initiatives dependent on individual champions, and career pathways that promote cybersecurity opportunities without giving learners a realistic way to gain experience. Estonia's strength was not a single program, but the alignment of digital competence frameworks, teacher support, organisational expectations, experiential learning and national cyber awareness. North American models similarly demonstrated that innovation has greater impact when frameworks, funding, educator development, practical infrastructure and industry participation operate as a connected ecosystem.

These findings have already influenced the Fellow's professional practice. He has expanded the use of simulations, real-world scenarios and challenge-based learning in diploma programs, designed and delivered two industry-informed cybersecurity courses, and encouraged student participation in Cyber Battle Australia, with two students progressing to the 2026 Grand Final. The Fellowship has also strengthened his research, leadership, public speaking and international networks, including acceptance into the EU CyberNet Expert Pool and participation in the California Cybersecurity Task Force Workforce Development and Education Subcommittee. Findings have been shared through the CyberMarvel Cyber Awareness Working Group, AVETRA 2026, EDUtech Australia 2026 and the Illuminate Forum 2026, with further dissemination planned through CyberCon 2026 and continued engagement with education, government, professional associations and industry.

The report proposes five connected recommendations. First, establish a time-limited national coordination group to align cybersecurity education, workforce development and accountability across schools, VET, higher education, government and industry. Second, define, map and pilot a baseline cybersecurity capability across VET, combining universal cyber awareness and safe digital behaviour with sector-specific occupational requirements. Third, create a tiered national VET educator capability initiative that includes paid release time, practical training, industry placements, mentoring, regional access and formal recognition where appropriate. Fourth, develop shared practical learning environments, including cloud-based cyber ranges, curated scenario libraries, Capture the Flag challenges and gamified activities mapped to units of competency. Fifth, strengthen connected pathways into cybersecurity work through articulation, recognition, mentoring, industry projects, supervised work-integrated learning and carefully governed cyber clinic pilots.

Together, these recommendations provide a practical reform sequence rather than a collection of stand-alone projects. They require national direction, state and territory implementation, provider leadership, industry participation, sustainable funding and evaluation that measures changes in educator practice, learner capability, pathway clarity, employment outcomes and equitable access. For Victoria, the opportunity is to lead through pilots that demonstrate how cybersecurity can be embedded across vocational disciplines, supported by capable educators and shared practical infrastructure. By acting now, Victoria can help move cybersecurity education from fragmented activity to an enduring system capability, one that protects learners and workplaces, strengthens industry resilience and prepares the workforce for a digital economy in which cyber responsibility belongs to everyone.

04
Fellowship Background

This fellowship was awarded in April 2025 in the first round of the 2025 Fellowship grants. The Fellowship examined how leading international systems integrate cybersecurity education, digital safety and workforce development across schools, vocational education, higher education, government and industry.

The Fellow's interest in this topic developed through his professional experience as a cybersecurity educator in the Vocational Education and Training (VET) sector. Since 2024, the Fellow has been teaching cybersecurity subjects within the Certificate IV and Diploma of Cybersecurity programs at Victoria University (VU). Through this experience, the Fellow observed that many learners enter cybersecurity programs without strong foundations in digital safety and core cyber concepts, while educators face limited professional learning time, resources, practical facilities and industry engagement. Early consultation showed that Australia's main problem is not a lack of initiatives, but poor coordination across policy, funding, curriculum, educator capability, infrastructure and evaluation. The Fellowship therefore examined the system conditions needed to connect teacher development, curriculum integration, practical learning, cross-disciplinary capability, workforce pathways and collaboration into a coherent cybersecurity education ecosystem.

Aim and Objectives

The aim of the Fellowship was to examine how internationally recognised systems integrate cybersecurity education and digital safety into education and training, and how educators are prepared and supported to deliver this learning effectively.

The objectives of the Fellowship include:

- understand how cybersecurity education is integrated into school and VET curricula in the United States, Canada and Estonia
- identify teacher capability and professional development models that prepare educators to teach cybersecurity, cyber awareness and digital safety
- explore how education systems, government agencies, industry partners and professional bodies collaborate to build cybersecurity capability and workforce pathways
- examine practical approaches, including cyber ranges, simulations, competitions, gamified learning and work-integrated learning models
- identify transferable principles and practical actions that could strengthen cyber awareness, educator capability and workforce development in Australia, with particular relevance to the Victorian VET sector

Relevance to Australia and the Victorian VET Sector

This Fellowship is closely aligned with the Australian Cyber Security Strategy 2023–2030, which recognises education, awareness and workforce development as essential to national cyber resilience. The Strategy is structured around six “Cyber Shields” designed to protect Australia’s digital ecosystem, several of which emphasise the importance of human capability, awareness and workforce development.

Figure 1. Cyber Shields - (Australian Government, 2023)

Cybersecurity is now a core capability across almost every digitally enabled industry, yet it is not consistently embedded or assessed across non-ICT VET qualifications. This can result in uneven learner preparedness and places additional pressure on educators and providers, particularly those with limited access to current resources, practical training environments, professional development and industry engagement. Strengthening cybersecurity capability across Victorian VET would improve learner safety, workforce readiness, employer confidence, organisational resilience and pathways into further study and employment. It would also position cybersecurity as both a specialist technical field and a foundational workforce responsibility relevant to all digitally enabled occupations.

Early Fellowship Research and Sector Consultation

The Fellowship used a qualitative, practice-based methodology combining Australian sector consultation, policy and program review, international expert engagement, organisational visits, conference participation and continuing virtual collaboration.

During the initial months of the Fellowship, the Fellow undertook preliminary research to understand the current landscape of cybersecurity education and teacher capability in Australia. This involved reviewing existing programs, policy initiatives and workforce development strategies related to cybersecurity education.

In 2025, the Fellow was invited by Rosemary Dore from the Australian Computer Society (ACS) to participate in the VET ICT Teacher Reference Group. As part of this initiative, the Fellow conducted a survey with VET educators to better understand the challenges faced by teachers in delivering cybersecurity education.

The survey identified several key issues. Teachers reported limited confidence in teaching technical cybersecurity skills, difficulty keeping up with rapidly evolving cyber threats and technologies, and limited access to teaching resources and curriculum materials. Teachers also highlighted structural barriers such as limited professional development opportunities, time constraints for upskilling, and limited engagement with industry. Teachers also indicated that improved professional development opportunities, access to updated teaching resources, collaboration with industry and practical training environments would significantly improve cybersecurity capability among educators.

These concerns provided the Fellow with an initial understanding of the broader system-level gaps affecting cybersecurity education. Although a range of initiatives exists, many appear to operate in parallel rather than as part of a coherent and coordinated education and workforce ecosystem. There are limited common capability expectations, inconsistent pathways for educator development, and insufficient alignment between policy, funding, curriculum, and implementation. This suggests that sustainable improvement requires coordinated policy direction, dedicated funding, and structured implementation support, rather than continued reliance on voluntary or isolated professional development activities. The Fellowship's international fieldwork was therefore designed to examine not only individual programs, but also the enabling policy, governance, funding, and institutional arrangements that allow successful initiatives to operate as part of a broader education and workforce system.

Engagement with Australian Initiatives

During the Fellowship, the Fellow also engaged with a range of conferences and professional events to gain insights into current developments in cybersecurity education and workforce capability.

In June 2025, the Fellow attended the EDUtech AU 2025 Conference in Sydney, where he gained valuable insight into emerging initiatives supporting cybersecurity education and digital safety in Australia. During the conference, the Fellow learnt about several initiatives aimed at strengthening educator capability and cyber awareness, including the ACS Cybersecurity Micro-credential for Educators, funded by the Queensland Government, which supports teachers in developing foundational cybersecurity knowledge and skills (ACS - Cybersecurity Micro-Credential, 2025). In addition, the Fellow was introduced to HackersJack, a cybersecurity knowledge platform designed to build cyber awareness and digital safety skills for learners of all ages, starting from children as young as eight years old through to teenagers (Hackersjack, 2022).

Furthermore, the Fellow also learnt that the University of Adelaide has developed a suite of Massive Open Online Courses designed to support Australian teachers in implementing the Australian Curriculum, particularly in STEM-related subjects. These online courses provide teachers with accessible professional learning, teaching resources and practical support to help integrate digital technologies and related topics, including cybersecurity and digital safety, into classroom teaching (CSER Group, n.d.). Besides, the Fellow also learnt about Cybermarvel, an online safety awareness program developed by the NSW Government to promote cyber safety education for students (Education, 2022).

Following these engagements, Mona Sidhu from the NSW Department of Education invited the Fellow to join the Cybermarvel Cyber Awareness Working Group. This working group functions as a centralised national forum connecting representatives from Departments of Education across Australia, focusing on initiatives related to cyber awareness and digital safety education in schools. Participation in this group provided the Fellow with an opportunity to engage with educators, policymakers and stakeholders involved in cybersecurity education across the country.

In addition to EDUtech 2025, the Fellow also attended AISA CyberCon in Canberra as well as in Melbourne during 2025. These events provided opportunities to engage with educators, policymakers, cybersecurity

professionals and researchers working on cybersecurity education initiatives and workforce development strategies internationally.

Figure 2. Faraz Khan - CyberCon Melbourne 2025

Engagement with Australian cybersecurity education and workforce initiatives has continued beyond the formal Fellowship period, enabling the Fellow to maintain connections with emerging programs, industry partners and practical learning opportunities. In July 2026, during Cyber Battle Australia 2026, the Fellow was introduced to Security Impossible, an Australian cyber range platform designed to support hands-on cybersecurity education for universities and TAFEs (Security Impossible, n.d.).

These continuing engagements with Australian initiatives have helped the Fellow remain connected with emerging approaches, partnerships and opportunities to strengthen cybersecurity education, educator capability and workforce development across Australia.

International Engagement and Study

The international component combined physical study visits and virtual engagement. An initial plan for the Fellowship included a visit to Estonia in July 2025 to study the country's widely recognised cybersecurity education and digital governance model. Estonia is internationally regarded as a leader in cybersecurity policy, digital infrastructure and cyber education.

Due to personal obligations, the Fellow was unable to travel to Estonia as originally planned. However, the Fellow contacted several Estonian stakeholders and requested that meetings be conducted online instead. These stakeholders were identified through desktop research, professional referrals and organisations directly relevant to the Fellowship objectives. Stakeholders included representatives from Riigi Infosüsteemi Amet (RIA) or National Cyber Security Centre of Estonia, the Ministry of Education and Research Estonia, and academics from Tallinn University. These virtual engagements proved highly valuable and provided important insights into Estonia's approach to cybersecurity education and national cyber capability development.

During this engagement process, the Fellow also became a member of EU CyberNet, a European Union initiative that connects cybersecurity professionals, policymakers, and researchers to strengthen international cooperation in cybersecurity capacity building. Participation in this network provided the Fellow

with opportunities to engage with experts and practitioners working on cybersecurity education, policy and workforce development across Europe.

To further explore international best practices in cybersecurity education, teacher training and workforce development, the Fellow travelled to the United States and Canada in December 2025. The United States was selected for its national cybersecurity workforce frameworks, extensive educator development initiatives and practical cyber range infrastructure. Canada was selected for its university–industry partnerships, workforce programs and community-based Cyber Clinic model. During this study visit, the Fellow engaged with a range of organisations involved in cybersecurity education, policy development, industry training and workforce initiatives. These were identified through desktop research, conference engagement and professional referrals. Additional contacts were established through recommendations made by initial participants.

In the United States, the Fellow interacted with organisations such as the National Initiative for Cybersecurity Education (NICE) at the National Institute of Standards and Technology (NIST), which provides national frameworks and resources for cybersecurity education and workforce development. The Fellow also connected with the Workforce Development and Education Subcommittee of the California Governor's Cybersecurity Taskforce, which focuses on strengthening cybersecurity education pathways across California.

The Fellow further explored education and training initiatives through engagement with organisations including Cyber Florida, NCyTE (National Cybersecurity Training and Education Center), US Cyber Range, TeachCyber, Cyber.org, Fortinet, and RING. These organisations provide a range of resources including cybersecurity curriculum development, cyber range training environments, teacher training programs, certification pathways and industry-supported education initiatives aimed at strengthening cybersecurity capability across schools, colleges and universities.

In Canada, the Fellow engaged with the Canadian Centre for Cyber Security, which plays a central role in national cyber resilience and workforce development initiatives. The Fellow also visited the Rogers Cybersecure Catalyst at Toronto Metropolitan University, a leading Canadian centre for cybersecurity training, workforce development and industry collaboration.

These engagements provided valuable insights into how leading countries are building cybersecurity education ecosystems that connect schools, higher education institutions, industry partners and government agencies.

In addition to these engagements, the Fellow attended the California Cybersecurity Education Summit in October 2025 (virtually) and participated in the NICE K–12 Cybersecurity Education Conference in Nashville, Tennessee in December 2025. These events brought together educators, policymakers, researchers and cybersecurity professionals working on national and regional initiatives to strengthen cybersecurity education.

Through these engagements, the Fellow gained a deeper understanding of international approaches to teacher training, curriculum integration, cyber awareness programs for students, and national frameworks supporting cybersecurity workforce development.

Following the study tour, the Fellow continued virtual meetings with contacts established in North America, as well as ongoing engagement with stakeholders across Australia. Evidence from interviews, meetings, survey consultation, program documents, policy sources and conference engagement was organised thematically around the Fellowship objectives.

Dissemination and Current Work

From early 2026, the Fellow has been engaged in organising dissemination sessions, stakeholder engagement activities and report writing to share insights from the Fellowship.

At the time of publication of this report, the Fellow is employed as a vocational education (VE) teacher specialising in cybersecurity at Victoria University (VU). The Fellow is part of the Centre of VU Transitions and primarily teaches within the Diploma of Cybersecurity programs.

The findings of this Fellowship aim to contribute to improving cybersecurity education in Australia by identifying practical approaches to support teachers, strengthen cyber awareness among students and help build a future-ready cybersecurity workforce. The findings identify transferable lessons and opportunities for Australia and not intended as a direct blueprint for reproducing another country's model.

05

Fellowship Learnings and Findings

Across the United States, Canada and Estonia, the Fellowship identified six interconnected findings. Effective cybersecurity education requires clear system direction and shared capability expectations; sustained and practical educator development; equitable access to realistic learning environments; the integration of cybersecurity across both ICT and non-ICT disciplines; clearer pathways between education and employment; and long-term funding, governance and evaluation arrangements. The international evidence also demonstrated that isolated resources or short-term programs are unlikely to create lasting change unless they are supported by capable educators, institutional ownership, industry participation and accessible implementation support. These findings provide the basis for considering how cybersecurity capability can be strengthened across Australian and Victorian VET while recognising the differences between international education systems and Australia's competency-based training model.

Study Visits in North America:

During the Fellowship, the Fellow met with a range of leading cybersecurity educators, researchers, and policy leaders across the United States and Canada. These discussions provided valuable insights into the development of cybersecurity education pathways, teacher capability, workforce development strategies, and the role of hands-on training environments. Although these conversations took place in different institutions and states, several consistent themes emerged regarding the opportunities and challenges associated with scaling cybersecurity education and developing a sustainable workforce pipeline.

National Frameworks and Coordination in Cybersecurity Education

A key theme that emerged during the Fellowship was the challenge of coordinating cybersecurity education within decentralised education systems. In the United States, education policy and curriculum development are primarily managed at the state level, which results in considerable variation in how cybersecurity education programs are implemented.

The Fellow met with Rodney J. Petersen, Director of Education and Workforce for the Applied Cybersecurity Division at the National Institute of Standards and Technology (NIST). Petersen explained that because the U.S. education system is highly decentralised, it is difficult to implement a single national cybersecurity curriculum. Dr Melissa Dark (founder of DARK Enterprises, Inc., a non-profit organisation focused on cybersecurity education development, assessment, research, and knowledge transfer) reinforced this perspective noting that cybersecurity education across the United States is shaped by a highly decentralised system, resulting in variation in policy mandates, curriculum provision, and levels of institutional support between states.

To address these challenges, a range of national frameworks and guidance documents have been developed to support greater consistency and alignment across the system. Resources shared by Dr Dark, including the 'Supplement to Cybersecurity Curricula (CSEC) 2017: Foundational Cybersecurity Content and Instructional Guidance for Secondary and Postsecondary Cybersecurity Education', provide structured guidance on core learning outcomes for introductory cybersecurity education. It aims to define foundational knowledge, support curriculum development, and enable stronger articulation between secondary and postsecondary education (Bishop et al., 2025).

Figure 3. Rodney J. Peterson and Faraz Khan

Petersen explained, initiatives such as the National Initiative for Cybersecurity Education (NICE) Framework provide common workforce standards, competency models, and shared terminology that help align education providers, government agencies, and industry stakeholders.

In addition to national frameworks, several organisations and initiatives provide practical implementation support. Petersen also highlighted the role of organisations such as Cyber.org, which is funded by the Cybersecurity and Infrastructure Security Agency (CISA) and supports cybersecurity education through curriculum resources, teacher professional development, and training programs. He further noted the contribution of national initiatives such as the College Board's Advanced Placement (AP) Cybersecurity course and the Teach Cyber program, both of which aim to strengthen cybersecurity education pathways within secondary education. The AP Cybersecurity course provides students with structured, college-level learning aligned with further study and career pathways, while Teach Cyber is a U.S.-based non-profit initiative that supports secondary school delivery through curriculum resources, assessment tools and educator support materials (AP Cybersecurity – AP Central | College Board, 2025; ARC Project – Teach Cyber, 2026).

Beyond these initiatives, the Fellow engaged with several other organisations supporting cybersecurity education, educator development and workforce pathways across the United States. This included a meeting with Michele Robinson, Senior Director and Principal Investigator of the National Cybersecurity Training and Education (NCyTE) Centre, a National Science Foundation-funded national centre dedicated to advancing cybersecurity education and workforce development (NCyTE Centre, 2022). Robinson explained that NCyTE plays a strategic role in strengthening the national cybersecurity workforce by collaborating with educational institutions, federal agencies, and industry partners to share best practices, develop educational resources, support faculty development, and address ongoing workforce shortages.

Together, these organisations and initiatives demonstrate the importance of coordinated national frameworks that bring together education providers, government agencies, industry partners, and

Figure 4. NICE Workforce Framework for Cybersecurity (National Initiative for Cybersecurity Careers and Studies, 2025)

professional associations to strengthen cybersecurity capability. While individual programs differ in their focus and delivery, collectively they contribute to a broader ecosystem that supports educator development, student pathways, curriculum innovation, and workforce readiness.

The broader implication is that Australia requires a shared architecture that establishes common language, foundational cyber capability expectations and pathway alignment while preserving contextualised delivery. In VET, national guidance could inform training product development, contextualised companion cyber resources, educator professional learning and articulation arrangements without displacing competency-based assessment or the responsibilities of registered training organisations.

Teacher Capability and Professional Development

Across several meetings, stakeholders emphasised that teacher capability remains one of the most significant barriers to expanding cybersecurity education.

Dr Melissa Dark explained that cybersecurity education in U.S. schools is still relatively new, having developed significantly over the past 10–15 years. Early efforts were driven by initiatives such as the GenCyber program, co-funded by the National Security Agency and the National Science Foundation, which delivered summer camps for both students and teachers across the country. These programs played a key role in raising awareness and building foundational capability, with an initial focus on supporting high school pathways aligned to industry certifications, followed by broader efforts to encourage engagement in cybersecurity as a field of study.

Figure 5. Dr Melissa Dark and Faraz Khan

Despite this progress, Dr Dark highlighted ongoing challenges in teacher preparation. She noted the absence of a standardised certification pathway for cybersecurity educators, with most states not offering a dedicated endorsement for teaching cybersecurity. As a result, educators from a wide range of disciplines, including business, English, and library sciences, are often tasked with delivering cybersecurity content. This lack of standardisation contributes to inconsistencies in curriculum delivery and depth of knowledge.

To address these challenges, Dr Dark highlighted the role of structured professional development initiatives such as the National Cybersecurity Teacher Academy (NCTA). This program provides in-service teachers with an 18-credit-hour qualification aligned with requirements for delivering dual credit courses and is offered in both intensive summer and extended formats. She noted that flexible delivery models and targeted financial support are important factors in improving participation and completion rates. These initiatives demonstrate the importance of scalable and consistent approaches to strengthening teacher capability in cybersecurity education.

Additional insights into teacher development were provided during the Fellow's meeting with Dr Candi Ring, who leads the Operation K12 initiative in collaboration with Cyber Florida and the Florida Centre

for Instructional Technology. Dr Ring described how Florida has expanded cybersecurity education in high schools over the past five years, including the introduction of structured course pathways and the availability of state-funded certification programs for teachers. She also shared examples of educators from non-technical disciplines successfully transitioning into cybersecurity teaching roles through targeted training and professional development.

More insights into teacher capability development were provided by Dr Shannon Beck, Director of the Virginia Cyber Range and the U.S. Cyber Range at Virginia Tech. Dr Beck highlighted the D.E.C.R.Y.P.T (Developing Educators in Cyber Readiness and Youth Pathway Training) program, a targeted professional development initiative designed to support secondary school teachers delivering introductory cybersecurity content. D.E.C.R.Y.P.T is sponsored by the U.S. Department of Defence Senior Military College Cyber Institute, the program provides educators with both foundational knowledge and practical teaching strategies across key areas such as cryptography, networking, and the Linux command line, alongside broader topics including ethics, cybersecurity careers, artificial intelligence, and emerging technologies (Decrypt, 2026).

The program incorporates a blended learning model, including pre-camp webinars followed by an intensive one-week residential training at Virginia Tech. A key feature of the program is the use of the Virginia Cyber Range, which enables participants to engage in hands-on laboratory activities and explore how practical cybersecurity concepts can be effectively translated into classroom teaching Participants are further supported through travel allowances and a completion payment, reflecting the program's structured and incentivised approach to professional learning (Virginia Cyber Range, n.d.). This initiative demonstrates the value of immersive, practice-based training models in strengthening teacher capability and confidence in delivering cybersecurity education.

The Fellow also explored curriculum and teacher support models through discussions with Brandon Sally, Curriculum Manager at Cyber.org, and Stacy Sinclair, Education Curriculum Specialist at Fortinet. Both organisations provide structured cybersecurity curricula designed to support teachers with varying levels of prior knowledge.

Cyber.org offers a K–8 cybersecurity curriculum that includes engaging, industry-aligned content across areas such as networking, coding, IT support, and foundational cybersecurity concepts. The program is supported through a range of professional learning opportunities, including virtual workshops, in-person training, and access to recorded sessions, enabling teachers to build confidence and capability in delivering the content.

Similarly, Fortinet's curriculum adopts a "train-the-trainer" approach, providing teachers with background knowledge, modular lesson plans, and flexible delivery methods tailored to different age groups and learning styles. The program includes interactive e-learning modules, assessments, and certification pathways, supporting educators to progressively develop their understanding while delivering cybersecurity education in the classroom.

These models demonstrate the importance of accessible, flexible, and well-supported curriculum design in enabling teachers, particularly those without a technical background, to effectively integrate cybersecurity into their teaching practice.

Further insights into teacher capability development were provided by Michele Robinson, who described the NCyTE Faculty Externship Program, which provides community and technical college educators with immersive industry-based professional development opportunities. Through this program, faculty undertake a minimum of 80 hours of placement within real-world cybersecurity environments, such as security

operations centres, to gain current knowledge of industry tools, practices, and workforce expectations. Participants are supported through structured agreements with industry partners and receive funding to facilitate their engagement. A key outcome of the program is that educators return to their institutions with updated industry insights, which are then integrated into curriculum and classroom practice. This model highlights the importance of strengthening links between education and industry to ensure that teaching remains aligned with evolving workforce needs.

Together, these insights highlight the importance of flexible professional development pathways that allow teachers from diverse backgrounds to develop cybersecurity teaching capability.

The most relevent lesson for Australian VET is that educator capability should be treated as essential workforce infrastructure rather than an optional responsibility left to individual teachers. The Fellowship found that Australian educators face barriers including limited confidence, insufficient time for professional learning, and inconsistent industry engagement, while international models demonstrate that effective capability development is structured, funded, practical, and sustained. A suitable Australian approach could combine contextualised companion cybersecurity resources for different VET disciplines, hands-on technical training, industry placements, train-the-trainer programs, and communities of practice, supported by paid release time, equitable access for sessional and regional educators, and funding for mentoring, travel, industry engagement, and classroom implementation.

Hands-On Cybersecurity Training Environments

Another key theme emerging from the Fellowship was the importance of practical learning environments that allow students to engage with realistic cybersecurity scenarios. Rodney J. Petersen cautioned against designing programs around specific vendors or technologies, noting that such approaches can quickly become outdated and may limit fairness and neutrality within the learning environment.

Figure 6. Faraz Khan at Rogers Cybersecure Catalyst

During the Fellow's visit to Canada, he met with Charles Finlay, founder of Rogers Cybersecure Catalyst, a not-for-profit organisation owned by Toronto Metropolitan University. Charles suggested that instead of trying to change the entire curriculum, which takes a long time, a good starting point would be cybersecurity clubs in schools. Finlay highlighted the Cyber Clinic model, which provides a practical, work-integrated learning model for developing cybersecurity capability. The Cyber Clinic delivers free cybersecurity support to under-resourced non-profit and community organisations, while simultaneously providing graduates with real-world experience (Catalyst Cyber Clinic, 2025).

The program is staffed by trained Catalyst graduates who, as consultants, work in teams to assess organisational needs and develop tailored cybersecurity action plans over a defined period. These teams are supported by experienced industry mentors, ensuring both the quality of outcomes for organisations and meaningful learning experiences for participants.

This model demonstrates the value of combining workforce development with community impact, enabling learners to apply their skills in real-world contexts while building professional experience. It highlights how

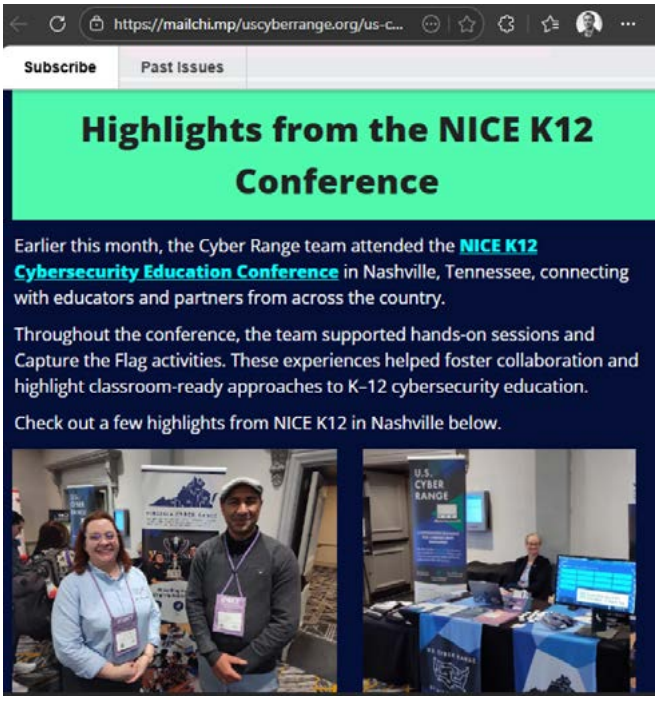


Figure 7. Screenshot from the U.S. Cyber Range newsletter featuring Faraz Khan and Dr Shannon Beck.

hands-on, service-based learning approaches can strengthen both technical capability and employability in cybersecurity.

While the Cyber Clinic model demonstrates the value of authentic, service-based learning, the Fellowship also identified scalable simulated environments as another important way to build practical capability. The Fellow learnt that shared infrastructure could expand access to hands-on cybersecurity education while reducing the technical and financial burden on individual institutions. Dr Shannon Beck explained that U.S. Cyber Ranges provide scalable cloud-based platforms that enable schools, colleges, and universities to deliver hands-on cybersecurity education through simulated cyber defence exercises and virtual lab environments.

These platforms allow students to safely explore vulnerabilities, network configurations, and malware behaviour within isolated systems, enabling learners to develop practical skills without exposing institutions to operational risks (U.S. Cyber Range, n.d.). Beck noted that the U.S. Cyber Range extends access nationally, providing educators with ready-to-use cyber labs aligned with industry frameworks. However, she also emphasised that building and maintaining cyber range infrastructure requires significant technical expertise and financial investment, which may be beyond the capacity of many smaller institutions. As a result, shared national cyber range platforms, available through subscription or access-based models, play a critical role in expanding access to practical cybersecurity training while reducing the technical and financial burden on individual providers.

This emphasis on practical learning was reinforced by Kristi Rice, a cybersecurity educator from Spotsylvania High School in Virginia and recipient of the 2021 Presidential Cybersecurity Educator Award. Rice described her approach as “thinking outside the box”, designing immersive and hands-on learning experiences that make complex cybersecurity concepts accessible and engaging for students. Through cyber ranges, Capture the Flag (CTF) competitions, and real-world cyber defence challenges, students do not simply study cybersecurity concepts, they experience them firsthand.

Collectively, these examples demonstrate that effective cybersecurity education extends beyond traditional classroom instruction and requires learners to engage in authentic, hands-on experiences. Whether through cyber clinics, cyber ranges, competitions, or simulated cyber defence environments, practical learning opportunities enable students to apply theoretical knowledge, develop technical and problem-solving skills, and gain insight into real-world cybersecurity practice.

The key insight for Australian VET is that practical cybersecurity training should be supported through shared, scalable and industry-relevant learning environments rather than requiring each provider to develop and maintain its own infrastructure. Although competency-based training already emphasises practical skills, access to current and secure cyber ranges, simulations and realistic scenarios remains uneven across providers. Shared cloud-based platforms, curated scenario libraries and regionally accessible training environments could improve consistency and equity, particularly where they are mapped to units of competency and supported by educator professional development. Cyber clinic models could also be piloted

to provide supervised real-world experience, provided that clear arrangements are established for scope, ethics, privacy, professional indemnity, quality assurance and industry mentoring. These models should complement, rather than replace, formal assessment and workplace-based learning.

Cybersecurity Across Disciplines and Industry Sectors

Several meetings highlighted the growing need to integrate cybersecurity education across a wide range of disciplines and industry sectors. Rodney J. Petersen emphasised the importance of developing foundational digital and AI literacy across all professions, not only within technology-focused careers, reflecting the growing relevance of cybersecurity knowledge in an increasingly digital society. Dr Melissa Dark also observed that, while there is growing interest in cross-disciplinary approaches, integration of cybersecurity across different subject areas remains limited in most U.S. states. She noted that many programs continue to be closely aligned with networking or vendor-based curricula, rather than being tailored to broader industry sectors. This highlights the need for more context-specific and locally relevant approaches that align cybersecurity education with regional economic priorities.

The Fellow learnt that cross-disciplinary cybersecurity is most effective when it is tailored to the specific risks and operational needs of different industries. Charles Finlay illustrated this through Rogers Cybersecure Catalyst, which operates two main programs: a Workforce Development Program focused on cybersecurity skills and training, and an Innovation Program that helps organisations integrate cybersecurity into their technologies and operational practices. Through the Innovation Program, the Catalyst works with multiple priority sectors identified by the government (Cyber Challenge, 2026). Finlay also noted that the program extends beyond general awareness training by providing organisations with hands-on technical support to strengthen their cybersecurity capabilities and improve overall security practices.

This focus on sector-specific application is further reflected in the use of industry-aligned cybersecurity assessment tools in the US. The Fellow also learnt about the free Cyber Security Evaluation Tool (CSET®), developed by the Cybersecurity and Infrastructure Security Agency (CISA) within the U.S. Department of Homeland Security. CSET® is primarily used by asset owners, operators, and cybersecurity professionals to evaluate the security posture of operational technology (OT), including industrial control systems, as well as information technology (IT) environments. By aligning assessments with recognised standards such as NIST SP 800-171, the tool highlights how cybersecurity practices are shaped by the specific requirements of different industry sectors, particularly within critical infrastructure environments (CSET, 2020). This reinforces the importance of sector-specific approaches to cybersecurity capability development.

The Fellow also learnt that embedding cybersecurity across disciplines requires close collaboration between educators and industry so that learning reflects the specific risks of each sector. Michele Robinson and Dr Kristine Christensen, Program Director for the National Community College Cybersecurity Fellowship Program at NCyTE, highlighted the Cybersecurity Across Disciplines initiative, which supports the integration of cybersecurity into fields such as healthcare, finance, transportation and energy. Through activities including the CyAD Summit, educators work with industry partners to develop curriculum addressing sector-specific cybersecurity challenges (CyAD, 2022). Robinson explained that NCyTE further supports this work through conferences, shared resources and targeted engagement, while travel funding and stipends enable broader participation by educators from non-cyber disciplines. Together, these initiatives demonstrate that cybersecurity is increasingly recognised as an essential capability across a wide range of professions.

Robinson, also explained that NCyTE works with more than 550 member institutions to expand cybersecurity education pathways, develop curriculum resources, and strengthen industry partnerships. She highlighted the Clark Cybersecurity Library, a national repository that provides free cybersecurity

curriculum resources. The Fellow explored the CLARK Cybersecurity Library and found more than 2,000 learning resources, including micro-modules, nano-modules, lesson plans, laboratory activities, and curriculum materials. The repository contains multiple collections designed to support different educational levels and disciplines (CLARK | Cybersecurity Library, 2024). For example, CLARK4Kids is an interactive K–12 curriculum collection that makes cybersecurity education engaging and accessible for young learners through hands-on activities, games, and real-world scenarios. In addition to school-focused resources, the library also contains specialised content for a range of sectors and disciplines. For instance, a search for medical device security returns multiple modules and nano-modules that can be readily integrated into relevant courses and training programs. The breadth and accessibility of resources available through the CLARK Cybersecurity Library demonstrate how national repositories can support educators while reflecting the growing recognition that cybersecurity is a capability relevant across a wide range of industries and professions.

Overall, the findings show that cybersecurity should not be treated as a standalone technical subject. Its greatest value comes from being embedded across disciplines, aligned with sector-specific risks and supported by industry-informed resources. The main takeaway for Australian VET is that cybersecurity capability should be embedded across industry qualifications rather than confined to ICT programs. Broad digital capability requirements may not adequately address the specific cyber risks faced in sectors such as health, manufacturing, community services, construction and logistics. Jobs and Skills Councils, employers and educators could work together to identify priority cybersecurity practices for each industry and determine whether these should be incorporated through revised units, electives, skill sets, implementation guidance or contextualised companion resources. A shared national repository could reduce duplication and support non-specialist educators, provided that resources are quality assured, regularly updated, accessible, mapped to training products and aligned with Australian regulation, workplace practice and competency-based assessment.

Education Pathways and Workforce Pipeline Development

Another important theme emerging from the Fellowship was the development of structured pathways that support students from school through to employment in cybersecurity careers.

The Fellow met with Dr. Keith E. Clement from Fresno State University, Chair of the Workforce Development and Education (WDE) Subcommittee of the California Governor’s Cybersecurity Task Force. Dr. Clement described the Cybersecurity Career Education Pipeline/Pathway Project (C3EP3), a statewide initiative designed to strengthen cybersecurity and AI workforce development through a coordinated education-to-employment pathway. During the Fellowship, the Fellow subsequently became a member of the California Cybersecurity Task Force WDE Subcommittee, providing valuable insight into the development of workforce and education strategies. At the time of submitting this Fellowship report, the California Cybersecurity-AI Workforce Development and Education Pathways Road Map and Curriculum Strategy Report was still under development. The emerging framework aims to align K–12 education, vocational training, higher education, industry certifications, and workforce development initiatives into a seamless career pathway. A key feature of the framework is its emphasis on experiential learning opportunities, including internships, apprenticeships, competitions, mentoring programs, and job shadowing, which help learners develop practical skills and transition successfully into cybersecurity careers. The initiative provides a useful model for building a sustainable cybersecurity talent pipeline and addressing future workforce needs.

Dr Clement also highlighted Fresno State’s Soft Start program, which provides beginner-friendly entry pathways into cybersecurity through linked certificate programs, free online courses, and paid internships. The program has already served more than 1,000 learners and aims to reduce barriers to entry for individuals interested in cybersecurity careers.

The Fellow learnt that strengthening the cybersecurity workforce also requires clear pathways for developing future educators. Dr Kristine Christensen illustrated this through the National Community College Cybersecurity Faculty Fellowship Program, which supports emerging cybersecurity educators through structured mentoring, technical training and supervised teaching experience. The program targets students nearing completion of undergraduate or postgraduate study and introduces teaching as a viable professional pathway.

Participants undertake a cybersecurity boot camp alongside workshops focused on pedagogy, classroom management, and curriculum design, and are required to complete supervised teaching placements. In addition, participants may work towards recognised educator certifications, such as the Microsoft Certified Educator credential. This program aims to address the shortage of qualified cybersecurity instructors by creating a clear and supported pathway for graduates to transition into teaching roles, thereby strengthening the long-term sustainability of the cybersecurity education workforce (NCyTE, n.d.).

Figure 8. Dr Kristine Christensen and Faraz Khan

The Fellow also learnt that strengthening cybersecurity capability also requires closer links between research, industry and practical innovation. Charles Finlay illustrated this through the Catalyst Fellowship Program at Rogers Cybersecure Catalyst, which supports both academic researchers and industry professionals to undertake cybersecurity projects addressing emerging strategic challenges.

The Catalyst fellowship operates across two streams - academic and industry, providing participants with opportunities to conduct original research, engage with industry partners, and contribute to innovation in cybersecurity practice. Fellows are supported through access to university resources, collaboration networks, and project-based funding, enabling them to bridge the gap between research and real-world application (Catalyst Fellowship Program, 2026). This model highlights the importance of integrating research, industry engagement, and workforce development, demonstrating how structured fellowship programs can contribute to building advanced cybersecurity capability and supporting the development of a skilled and adaptable workforce.

The Fellow learnt that structured school-to-work pathways can strengthen cybersecurity workforce development, but their effectiveness depends on consistent access across jurisdictions. Dr Melissa Dark illustrated this through Career and Technical Education (CTE) pathways in the United States, which are supported through federal block grants and organised across 16 national career clusters, with cybersecurity generally positioned within the broader digital technology cluster. However, the availability and structure of cybersecurity pathways vary significantly across states and schools. While some jurisdictions offer dedicated pathways, others provide only limited exposure, resulting in uneven access for students. This lack

of consistency presents challenges for developing coherent pathways from school education into further study and employment.

In response to this uneven access, the Fellow learnt that nationally recognised programs can help create more consistent pathways from secondary education into further study and employment. At the NICE K–12 Cybersecurity Education Conference, Andrew Tucker, Senior Director of the Advanced Placement Program at the College Board, presented the development of the AP Cybersecurity course. This course is designed to align with introductory university-level cybersecurity studies and provides high school students with the opportunity to engage in college-level learning while still in secondary education. The course focuses on core cybersecurity concepts, including vulnerabilities, threats, and defence strategies across multiple domains, and is aligned with the NICE Workforce Framework. As part of the College Board's Career Kickstart initiative, the course is also developed in collaboration with industry to support career readiness.

A notable feature of the Advanced Placement model is that students who achieve qualifying examination scores may be eligible to receive university credit or advanced standing at participating higher education institutions. This approach enables students to undertake university-level learning while still at school and, in some cases, reduce the time and cost required to complete a degree by receiving recognition for prior learning. By creating a direct pathway from secondary education into higher education, the AP Cybersecurity course strengthens the cybersecurity talent pipeline and provides students with a clearer transition into further study and future careers in the field (AP Cybersecurity College Board, 2025). This model demonstrates how curriculum alignment between schools, universities, and industry can support both educational progression and workforce development.

Complementing the AP Cybersecurity pathway, the Fellow learnt that scalable online programs can extend access to schools that do not yet have the capacity to offer dedicated cybersecurity courses. At the NICE K–12 Cybersecurity Education Conference, the RING (Regions Investing in the Next Generation) program was presented as an online high school course that provides structured content, lesson plans and hands-on activities for schools without established cybersecurity programs. Delivered at no cost through government funding and academic partnerships, the program aims to expand access to cybersecurity education while guiding students towards future career pathways. Its focus on ethics, professional identity, and career exploration highlights the role of early engagement in building a sustainable cybersecurity workforce (Center to Advance CTE, n.d.).

Building on these pathway models, the Fellow learnt that education and training decisions should also be guided by reliable labour-market intelligence. In discussions with Dr Davina Pruitt-Mentle, Lead for Academic Engagement in the National Initiative for Cybersecurity Education at NIST, and Donna Woods, Head of Cyber AI Partnerships at Work Education California, the Fellow explored tools such as CyberSeek, CyberStates and O*NET. These platforms provide data on workforce demand, skills shortages, certification requirements and long-term employment trends. The discussion highlighted how educators, workforce agencies and policymakers can use this evidence to align curriculum, training pathways and program investment with genuine employment opportunities. The key insight was that cybersecurity pathways are most effective when they respond to current and emerging workforce needs, strengthening the connection between education, economic priorities and employment outcomes.

Collectively, these initiatives highlight the importance of a coherent and multi-layered approach to cybersecurity education pathways. These examples demonstrate that effective workforce development requires not only early engagement, but also aligned pathways that connect secondary education, vocational training, higher education, and industry. Such integrated models are critical for building a sustainable and future-ready cybersecurity workforce.

The significant lesson for Australian VET is that strengthening cybersecurity pathways requires more than increasing course enrolments; learners need clear entry points, recognition of prior learning, stronger articulation between schools, VET and higher education, access to mentoring and work-integrated learning, and realistic pathways into entry-level employment. Pathway planning should draw on existing Australian labour-market resources, including AUCyberExplorer.au, which provides information on cybersecurity workforce demand, skills and career pathways, together with Jobs and Skills Australia and state and territory workforce data. Education providers, government and industry could use this evidence to align programs with regional demand and monitor transitions from school into VET, course completion, articulation, participation in placements and employment in relevant roles.

Sustainability and Workforce Development Challenges

While many promising initiatives are emerging, several stakeholders emphasised the challenges associated with sustaining cybersecurity education programs over time. Rodney J. Petersen noted that many programs initially funded through government grants struggle to continue once funding cycles end. Without long-term funding models and institutional commitment, programs risk losing momentum before they can produce meaningful workforce outcomes.

The Fellow also learnt that sustainability extends beyond program funding to the transition from education into employment. Petersen observed that many entry-level cybersecurity roles require substantial experience and multiple certifications, creating barriers for students and recent graduates. He emphasised that the solution is not to lower professional standards, but to provide learners with structured opportunities to gain the experience needed to enter and progress within the workforce.

These workforce-entry barriers are compounded by uneven access to cybersecurity education. Dr Melissa Dark referred to the CyberSupply research project and noted that only a relatively small proportion of U.S. high schools offer dedicated cybersecurity programs (CyberSupply, 2023). Differences in curriculum provision, educator capability and resource availability between states further limit access and make it difficult to establish consistent pathways from school into further study and employment.

Dr Dark explained that the absence of aligned structures across the education system contributes to fragmented implementation and restricts the ability to scale successful programs. Together, these challenges demonstrate that a sustainable cybersecurity workforce pipeline depends on more than creating individual courses or short-term initiatives. It requires coordinated funding, consistent access, institutional ownership and stronger collaboration between government, industry and education providers.

The key transferable lesson for Australian VET is that promising cybersecurity initiatives should not remain dependent on short-term grants, individual champions or temporary partnerships. Programs that demonstrate value need a planned transition to institutional ownership or recurrent funding so that educator expertise, industry relationships and learner access are sustained. Sustainability should therefore be built into pilots from the outset by identifying ongoing costs, provider capacity, regional access, evidence of learner and employer benefit, and responsibility for continuation.

Cyber Awareness and Cyber Hygiene

Several discussions also emphasised the importance of cybersecurity awareness and digital safety education across the broader population. Rodney J. Petersen highlighted the need for cyber safety, cyber awareness, and cyber ethics to be introduced from an early age and reinforced throughout tertiary education. Dr Melissa Dark further noted that, in many schools in the US, foundational cybersecurity awareness is introduced through broader subjects such as consumer sciences or digital literacy, rather than through dedicated courses. This reflects the early stage of cybersecurity curriculum development and the

Figure 9. Dr Candi Ring and Faraz Khan

ongoing need to strengthen structured pathways across all levels of education.

This emphasis on early cyber awareness was also reflected in discussions with Stacy Sinclair, Education Curriculum Specialist at Fortinet. Sinclair highlighted the Fortinet Security Awareness Curriculum, a free downloadable resource designed for students aged 8–11, 12–14, and 15–18 years. The curriculum provides educators with ready-to-use lesson plans, classroom activities, and awareness resources covering topics such as online safety, cyber hygiene, password security, phishing, privacy, and digital citizenship. The availability of age-appropriate resources across multiple year levels demonstrates how industry can support schools in embedding cybersecurity awareness and responsible online behaviour throughout a student's educational journey (Security Awareness Curriculum | Fortinet, 2025).

While curriculum resources can support classroom delivery, the Fellowship identified examples of how government policy can be used to drive the implementation of cyber safety education at scale, ensuring that digital safety becomes a core component of student learning. Dr Candi Ring described how Florida has introduced legislation requiring all students to complete one hour of cyber hygiene training, reflecting growing recognition of the importance of digital safety education. She also highlighted the Virtual Cyber Program developed through a partnership between Cyber Florida and Teaching Digital Natives, which provides no-cost cybersecurity curriculum resources to support Florida public schools in meeting these legislative requirements (Cyber Florida, n.d.). In addition, Dr Ring discussed initiatives designed to engage younger learners through interactive cybersecurity camps and activities that introduce cybersecurity concepts in accessible and engaging ways.

The Fellowship also found that successful cyber awareness initiatives depend on educators having access to concise and practical professional learning. During the visit to Canada, the Fellow also met with members of the Cyber Skills Development Team at the Canadian Centre for Cyber Security, including Alysha St John, Cyber Engagement Advisor, and Jonathan Joynt, Instructor at the Canadian Centre for Cyber Security. St John and Joynt described the team's work in supporting cybersecurity education and awareness initiatives across Canada. One of their initiatives is a free online course titled 'Introduction to Cyber Security for Educators'. The course is designed to provide teachers with a foundational understanding of cybersecurity concepts and strategies for protecting students in digital learning environments. The self-paced course takes approximately one to one and a half hours to complete and includes interactive learning activities, knowledge checks, and a final assessment. Since its launch, the course has attracted hundreds of participants and has been well received by educators seeking accessible professional development opportunities (Canada, 2025). According to St John and Joynt, the program demonstrates the value of concise, accessible training resources that can be integrated into teachers' busy schedules.

This focus on accessibility was further reflected in initiatives led by Rogers Cybersecure Catalyst. CyberStart Canada is a free online program that introduces young people aged 16–24 to foundational

cybersecurity concepts through interactive challenges and guided learning. In addition, the organisation provides free Cybersecurity for K–12 Educators resources, offering curriculum-linked lessons on digital citizenship, cyber safety, and online wellbeing. Covering all school year levels, these resources include ready-to-use teaching materials that support educators in delivering cyber awareness and cyber hygiene education across the curriculum (Rogers Cybersecure Catalyst, n.d.).

Collectively, these examples demonstrate a growing international recognition that cybersecurity and digital safety are essential life skills for all learners, not just those pursuing cybersecurity careers. The initiatives observed across the United States and Canada highlight the importance of embedding cyber awareness, cyber hygiene, and responsible digital citizenship throughout the education system while also providing educators with accessible professional learning opportunities.

A overarching lesson for Australian VET is that a baseline of cyber awareness and safe digital behaviour should apply across all disciplines, not only to learners enrolled in cybersecurity qualifications. This baseline should be reinforced within occupational contexts so that learners understand the cyber risks associated with activities such as handling health information, managing customer data, and using artificial intelligence tools in their field. A one-off awareness module would be insufficient; providers require adaptable resources, educator guidance and opportunities to revisit and assess safe practice throughout a qualification. Any national approach should build on existing digital literacy and online safety initiatives, avoid duplication, and be accessible and culturally responsive to learners with different levels of digital experience.

Toward a Flexible and Integrated Cybersecurity Education Ecosystem

Overall, the North American findings demonstrate that an effective cybersecurity education ecosystem requires five interconnected system functions: common frameworks that provide consistency; sustained educator capability development; shared curriculum resources and practical training infrastructure; clear education-to-employment pathways supported by work-integrated learning; and ongoing partnerships between government, industry and education providers. These functions must operate together. National standards and competency frameworks can provide coherence, but they will not improve learner outcomes without capable educators, accessible infrastructure and flexible delivery models that can respond to emerging technologies and evolving cyber threats. Similarly, practical programs and innovative curriculum initiatives are unlikely to achieve broad impact without recognised pathways, institutional ownership and sustainable funding.

The findings also identify risks that Australia should avoid, including over-reliance on vendor-specific content, unequal access between well-resourced and under-resourced providers, fragmented state or institutional initiatives, short-term projects without continuation plans, and workforce pathways that promote opportunities without providing supported entry points into employment. The key transferable lesson is therefore that Australia should not seek to replicate a single international initiative. Instead, it should develop a coordinated portfolio of reforms that strengthens educator capability, expands access to practical learning environments, embeds cybersecurity across disciplines, improves pathways between education and employment, and supports sustained collaboration across the system.

Virtual Engagement with Estonian Cybersecurity Stakeholders:

Estonia began developing its digital education system in the 1990s through the Tiger Leap program, which provided schools with computers, internet access, teacher ICT training, and digital learning materials. Later initiatives such as Tiger Leap Plus improved ICT skills of teachers and students and supported collaboration through platforms like the School Life portal. In 2012, the ProgeTiger and IT Academy programs were introduced to strengthen digital skills, programming education, and higher ICT education. These initiatives

support Estonia's Lifelong Learning Strategy 2020, which promotes digital technology and digital competence across the education system (Education Estonia, n.d.).

Although the Fellow was unable to undertake a physical visit to Estonia as originally planned, a series of virtual engagements were conducted with leading experts from government agencies, universities, and international cybersecurity initiatives. Estonia is widely recognised as a global leader in digital governance and cybersecurity, and these discussions provided valuable insights into how cybersecurity is embedded across its education system and broader society.

National Approach to Cybersecurity and Digital Competence

The Fellow learnt that Estonia's approach to cybersecurity education is strengthened by embedding it within a broader national digital competence framework. Discussions with Tiina Pau, Expert-Coordinator at the National Cyber Security Centre of Estonia (RIA), and Elyna Heinmäe, Visiting Research Fellow at the School of Digital Technologies at Tallinn University, highlighted how cybersecurity is integrated systematically across the education system.

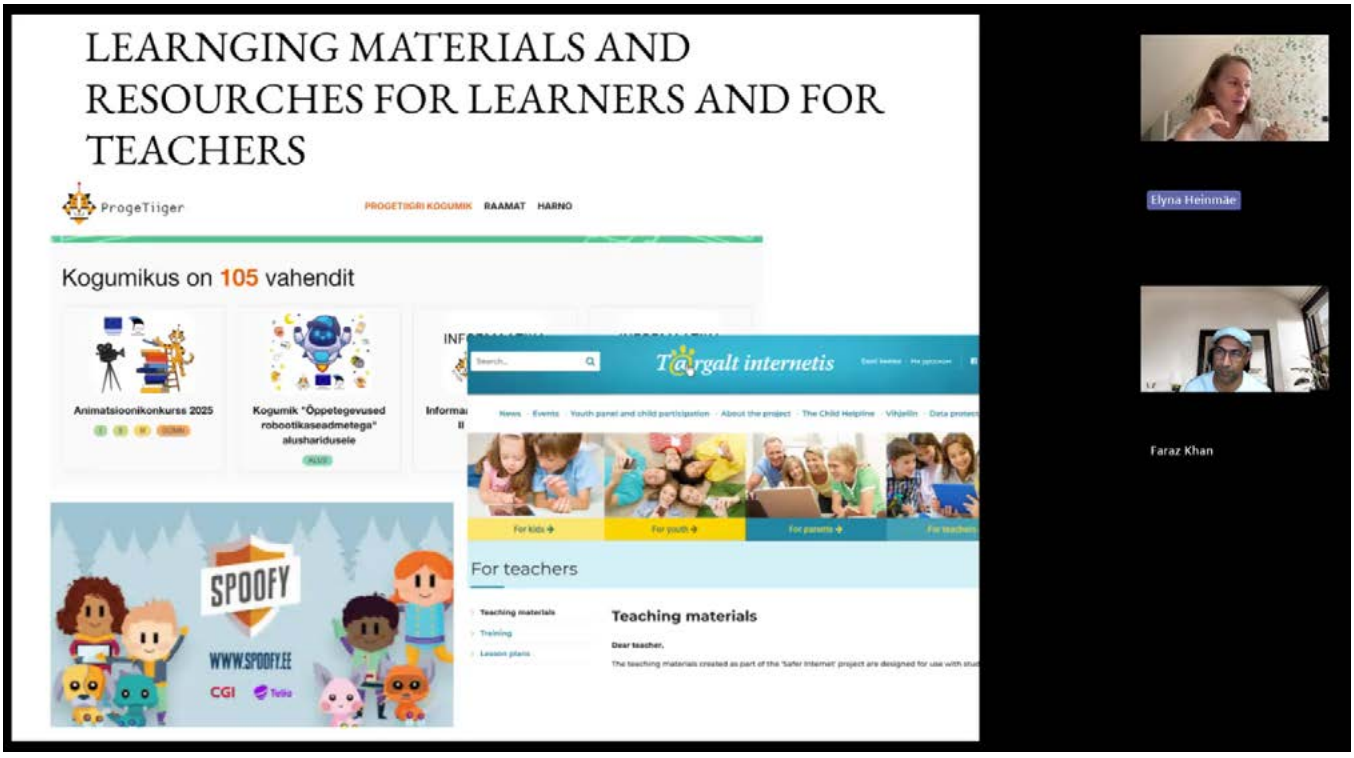


Figure 10. Faraz Khan and Elyna Heinmäe in a virtual meeting

Cybersecurity in Estonia is not delivered as a standalone subject but is embedded within the national curriculum as part of digital competence, one of the eight general competencies. This approach ensures that cybersecurity awareness and digital skills are developed progressively across all levels of education, from early childhood through to secondary schooling.

Heinmäe further explained that Estonia utilises structured digital competence frameworks (Digital Competence - Estonia, n.d.) to guide both teacher capability development and student learning outcomes. Estonia's teacher digital framework is primarily based on Digital Competence Framework for Educators (DigCompEdu, n.d.) and it has six dimensions. These include professional engagement, digital resources, teaching and learning, assessment, empowering learners, and facilitating learners' digital competence. The framework provides a structured approach for developing teachers' capability to integrate digital

technologies into teaching while also supporting students to develop the digital skills, digital citizenship, and cybersecurity awareness required for participation in a digital society.

Figure 11. Teachers' Digital Framework (Pozogina, 2023)

This structured approach is mirrored in Estonia's student digital competence framework, which is adapted from DigComp 2.1. It includes five dimensions: information and data literacy, communication and collaboration, digital content creation, safety, and problem-solving. Because these competencies are embedded across the curriculum, students develop cybersecurity awareness and responsible technology use as part of their broader learning rather than through isolated activities.

Figure 12. Students' Digital Framework (Pozogina, 2023)

The key transferable insight from Estonia for Australia is the value of positioning cybersecurity within a broader, progressive digital competence framework rather than treating it as a separate or isolated topic.

For Australian VET, this does not mean directly adopting Estonia's model, as governance arrangements, curriculum responsibilities and provider settings differ significantly. A more practical adaptation would be to define a baseline cyber capability that develops across the education pipeline and is then contextualised to different occupations, industries and qualification levels. To be effective, this framework would need alignment between learner expectations, educator capability, teaching resources and assessment guidance, supported by mapped examples, professional learning and evidence of how cyber capability progresses from school into VET, higher education and employment.

Teacher Capability and Professional Development

A consistent finding across the Estonian engagements was that effective cybersecurity education depends on sustained teacher capability and practical implementation support.

Pau described the role of educational technologists, who are embedded within most schools to support teachers in integrating digital skills and cybersecurity concepts into classroom practice. These specialists play a critical role in bridging the gap between policy and implementation. Heinmäe noted that the availability of educational technologists within schools is influenced by the budget constraints of the respective municipality.

The Fellow also learnt that Estonia uses scalable professional learning models to extend digital safety capability across schools. Pau highlighted initiatives such as the Digital Safety ABC in My School program (Kerli Kuusk, 2023) which adopts a cascade model of professional learning. In this program, selected teachers receive intensive training in digital safety and are then responsible for sharing this knowledge with their colleagues within their schools. This approach supports scalable and sustainable professional development.

The Fellow further observed that a range of structured professional development programs further support the development of teacher digital competence in Estonia. Initiatives such as the Digital Key program focus on helping subject teachers integrate digital technologies into their teaching practice, aligning with the national student digital competence framework. The Digital Accelerator program provides a more comprehensive, six-month development pathway for school teams, offering both foundational and advanced training based on teachers' existing capabilities. This program also includes digital leadership training for school management and ongoing coaching, with external evaluation of school progress after one year. In addition, shorter professional learning opportunities, such as the Digital ABC sessions, provide targeted training on the use of widely adopted digital platforms and tools (Digital Competence: Empowering Teachers and Students - Estonia, n.d.).

Heinmäe reinforced the importance of continuous learning, noting that Estonia provides a range of government-funded training opportunities, including online courses, face-to-face workshops, and postgraduate programs. Tallinn University, for example, offers a specialised master's program for educational technologists, further strengthening teacher capability in digital and cybersecurity education. Together, these approaches demonstrate a coordinated effort to ensure that educators are equipped to deliver cybersecurity-related content effectively across the curriculum.

The critical insight from Estonia for Australia is that successful cybersecurity education requires implementation support that connects policy expectations with classroom and training practice. While a direct replication of Estonia's educational technologist model may not be financially feasible across Australian schools and VET providers, particularly in regional areas, the principle could be adapted through regional capability hubs, shared specialist advisers, provider-based digital and cyber learning leads, and communities of practice that support multiple teaching teams. Estonia's cascade model also offers a useful scalable approach, but only where train-the-trainer programs include high-quality initial training, protected

time for peer support, quality assurance, follow-up activities and ongoing access to specialist expertise, rather than assuming that knowledge will automatically spread through an organisation.

Cybersecurity Integration Across Education and Society

The Fellow learnt that Estonia treats cybersecurity not only as an educational issue, but as a shared societal and organisational responsibility.

During the meeting with Meidi Sirk, Associate Professor of Vocational Education at Tallinn University, it was noted that cybersecurity is integrated into education through digital competence, critical thinking and awareness of secure practices in everyday contexts. Sirk also explained that cybersecurity is incorporated into national defence education at the secondary school level. Students learn about the functioning of the state, civic responsibilities, and the role of cybersecurity in maintaining national resilience and independence. This reflects Estonia's strategic emphasis on cybersecurity as a component of national security.

This whole-of-society approach is reinforced through legislation and organisational requirements. Pau highlighted the role of Estonia's Cybersecurity Act, which serves as a key policy driver in embedding cybersecurity practices across public sector organisations, including educational institutions. The legislation requires government and local administration bodies to comply with the Estonian Information Security Standard, which sets expectations for organisational cybersecurity practices (Estonian Information Security Standard, 2022).

A significant component of this model is the requirement for employee training in cybersecurity hygiene. Organisations, including schools and vocational institutions, must ensure that staff are aware of cybersecurity risks and are provided with appropriate training where necessary. This requirement reinforces cybersecurity as a shared organisational responsibility rather than a purely technical function.

Pau also highlighted the introduction of a national cybersecurity awareness test known as Kübertest, developed by Information System Authority (RIA). Kübertest is designed to raise and sustain cybersecurity awareness among employees, particularly within government agencies, while remaining accessible to a broader audience (Cyber Test, 2023). By leveraging a familiar learning platform, the initiative enables scalable and continuous engagement with cybersecurity concepts.

Together, these measures demonstrate Estonia's integrated approach to cybersecurity, where legislative requirements, organisational practices, and continuous training initiatives work collectively to strengthen cyber resilience across both education and the wider public sector.

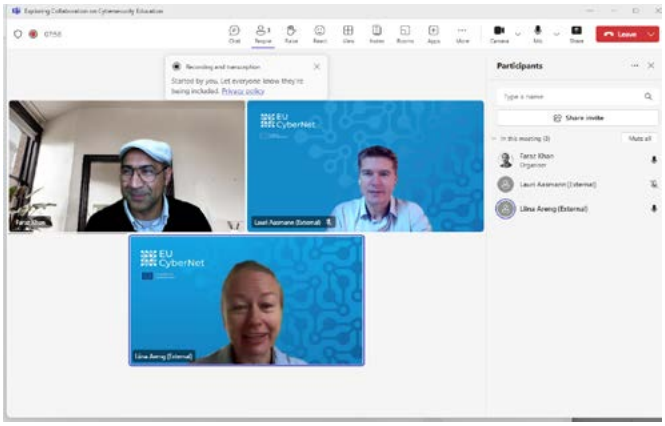


Figure 13. Virtual Engagement - Liina Areng, Lauri Aasmann and Faraz Khan

The Fellow gained further insights from Lauri Aasmann, Training and Services Lead, and Liina Areng, Director at EU CyberNet. They explained that EU CyberNet, a European Union-funded initiative, supports cybersecurity awareness and literacy at both national and international levels. Its activities include regular cyber hygiene testing for government employees and critical-sector organisations, as well as tailored training programs developed with local and international partners. Areng also noted that EU CyberNet provides training for vocational teachers and organises short intensive courses, annual winter schools and summer schools for members of its expert network.

These examples show that cybersecurity education in Estonia extends beyond formal curriculum and is reinforced through legislation, staff development, organisational practice and national capability-building initiatives.

The broader insight for Australia is that cyber capability is strengthened when education policy, organisational practice and workforce expectations are mutually reinforcing. Cyber capability should not be treated only as a curriculum issue, it also needs to be part of how education providers operate as organisations. For Australian VET, this means recognising that VET providers teach future workers, employ staff, manage digital systems and hold sensitive learner information. Therefore, staff cyber awareness, organisational cyber governance and cybersecurity teaching should be connected, rather than managed separately as compliance, IT or curriculum tasks. Because Australia's education and training responsibilities are shared across national, state and provider levels, the aim should not be to copy Estonia's single national testing approach. Instead, Australia could adopt the broader principle of setting clear expectations, providing accessible training, reinforcing safe practice over time and measuring progress. National and state initiatives should support provider-level cyber risk management and avoid reducing cybersecurity to a once-a-year compliance activity.

Experiential and Non-Formal Learning Pathways

The Fellow learnt that Estonia uses game-based, simulation-based and non-formal learning to build cybersecurity awareness, practical capability and interest across different stages of education.

During discussions with Peadar Charles Callaghan, Junior Research Fellow at Tallinn University, the Fellow explored how serious games and simulations can develop both technical and non-technical cybersecurity skills. Callaghan highlighted initiatives such as SuperCyberKids, which provides structured lesson plans and interactive activities designed to build cybersecurity awareness (SuperCyberKids, 2026). He also discussed Spoofy, an educational game that teaches children about online safety, responsible digital behaviour and risks associated with smart devices. These examples demonstrate that well-designed games can make complex cybersecurity concepts accessible and engaging for learners of different ages.

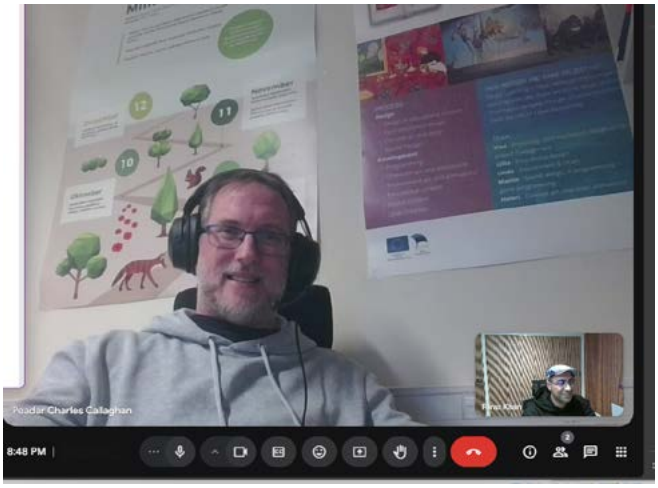


Figure 14. Peadar Charles Callaghan and Faraz Khan in a virtual meeting

The Fellow gained further insights through correspondence with Dr Birgy Lorenz, Senior Scientist at the Centre for Digital Forensics and Cyber Security at Tallinn University of Technology. Lorenz highlighted Estonia's broader ecosystem of non-formal learning, including national competitions such as CyberPin, CyberCracker, CyberDrill and CyberSpike. These initiatives provide progressive learning opportunities from primary school through to advanced levels and include cryptography, problem-solving, open-source intelligence and Capture the Flag challenges (CyberSpike, 2026).

Advanced learners are further supported through CyberCamps, which provide intensive training, mentoring and exposure to industry environments. These programs often involve private-sector and international partners and create pathways into competitions such as the European Cyber Security Challenge. Lorenz also highlighted initiatives supporting women in cybersecurity, demonstrating how non-formal learning can contribute to both talent development and greater diversity.

Together, these examples show how experiential learning can engage learners early, identify emerging talent and create progression routes into formal education and cybersecurity careers. For Australia, game-based and challenge-based learning can strengthen the school-to-VET pipeline by helping students develop confidence, interest and foundational cyber capability before entering specialist programs.

For Australian VET, non-formal learning can also complement formal qualifications through Capture the Flag activities, simulations, cyber clubs and supported professional learning labs. Cyber Battle Australia provides a relevant local example of how learners can apply cybersecurity skills in a practical environment. However, this approach could also be extended to educators through teacher-focused cyber challenges or professional learning labs. These should not be designed as high-pressure competitions, but as supported capability-building activities where teachers experience practical cybersecurity tasks, build confidence and translate challenge-based learning into classroom practice. For Australian VET, this could strengthen educator capability, support communities of practice and help trainers design more engaging, scenario-based learning experiences for students.

Integrated system finding from Estonia

Viewed as a whole, Estonia demonstrates that cybersecurity education is most effective when it is embedded within a broader digital capability system rather than treated as a separate curriculum add-on. Its approach connects a progressive digital competence framework with teacher capability development, specialist implementation support, organisational cyber requirements, experiential learning and non-formal talent pathways. The strength of the model is not any single initiative, but the way these elements reinforce one another. Learner expectations are supported by educator capability, practical resources, engaging learning activities and wider organisational cyber awareness.

For Australia, the transferable lesson is not to replicate Estonia's model directly, but to apply its system design principle. A practical Australian adaptation would define a baseline cyber capability that develops from school into VET, higher education and employment, while allowing this capability to be contextualised across occupations, industries and qualification levels. For Australian VET, this would require national direction, state and territory implementation, provider-level support, mapped teaching and assessment resources, professional learning, practical learning opportunities and mechanisms to measure progress over time. The Estonian example reinforces that cyber capability must be connected across curriculum, educator development, organisational practice and learner pathways, rather than delivered through isolated activities or one-off compliance training.

06

System-Level Issues, Recommendations and Next Steps

The Fellowship findings indicate that the principal Australian challenge is not an absence of activity. Cybersecurity qualifications, professional learning, school initiatives, industry resources and awareness programs already exist. The system-level weakness is that these elements are not consistently connected through enduring policy, funding, governance, curriculum, capability and evaluation arrangements. This section therefore distinguishes the problems that can be addressed by an individual educator or provider from those that require coordinated sector or system action.

What is not working in the current system

1. Fragmented policy and accountability:

Cybersecurity workforce, online safety, school curriculum, VET, higher education and industry initiatives are often developed through different policy channels. There is no consistently visible mechanism that assigns responsibility for aligning these activities across the learner and workforce pipeline. This can produce duplication in some areas and gaps in others, while providers and educators remain uncertain about which framework or priority should guide implementation. The consequence is variable access and a reliance on local leadership rather than dependable system settings.

2. Funding is frequently short-term and program-specific:

The international evidence and Australian consultation both show the limits of grant-dependent activity. Funding often supports the development or launch of a resource, pilot or platform but does not necessarily provide for educator release time, technical maintenance, mentoring, evaluation or continuation. Smaller, regional and community-based providers are less able to absorb these costs. The result is a cycle in which innovation is demonstrated but not embedded.

3. Curriculum and training product responsiveness is uneven:

Cybersecurity changes faster than formal review cycles. Specialist qualifications may be updated, but the cyber implications of digital work are not consistently addressed across non-ICT training products. Providers can contextualise delivery, yet contextualisation alone cannot correct unclear or absent national expectations. Without a structured mechanism for identifying occupational cyber risk, workers may complete qualifications without practising the secure behaviours required in their industries.

4. Educator capability is not treated as core workforce infrastructure:

Educators are central to embedding cybersecurity capability, but they are not always given the support needed to teach it confidently and contextually. This is especially important when cyber units appear in non-ICT qualifications such as business, library services, legal services, tourism or community services. In these areas, educators may have strong discipline knowledge but limited cyber expertise, and generic technical training may not translate into practical, occupation-specific teaching. When professional learning, industry currency and teaching resources depend on local initiative or individual effort, implementation becomes inconsistent and difficult to sustain.

5. Access to practical learning environments is unequal:

Cyber ranges, simulations and authentic scenarios are essential for applied capability, but platforms require funding, technical expertise, content maintenance and educator support. Well-resourced providers can create strong environments while others rely on limited or outdated laboratories. This affects both specialist cybersecurity learners and students in other disciplines who would benefit from safe, contextualised practice.

6. Education-to-employment pathways remain discontinuous:

Schools, VET, universities, certifications, competitions and employer recruitment often operate as parallel pathways. Recognition, articulation and work-integrated learning are not consistently available, and entry-level roles may demand experience that new graduates have had little opportunity to acquire. This weakens the return on training investment and can disadvantage learners without professional networks.

7. A cross-disciplinary cyber baseline is not consistently defined:

Cybersecurity is relevant to every digitally enabled occupation, but there is no consistently applied baseline that explains what all VET learners should know and do, and what additional practices are required in particular sectors. This leads either to omission or to generic awareness content that is not connected to occupational decisions, assessment or workplace responsibility. Even where cyber is included, assessment may rely on written responses rather than authentic workplace scenarios, simulations, incident response activities or role-based decision-making that demonstrate practical cyber capability.

8. Evaluation is focused more on activity than system change:

Programs commonly report enrolments, attendance, resource downloads or events. These are useful outputs but do not show whether educator practice changed, learners developed capability, pathways improved, employers observed greater readiness, or access became more equitable. Without shared measures and long-term tracking, it is difficult to compare programs, direct funding or decide which pilots should be expanded.

9. Cybersecurity inclusion is often optional rather than assured:

Although cybersecurity units are increasingly appearing in some non-ICT qualifications, their inclusion does not always mean that all learners will develop cyber capability. In many cases, cyber units are listed as electives or imported electives rather than core requirements. This means delivery depends on provider choice, local expertise, timetabling, funding and perceived relevance. As a result, two learners completing the same qualification may have very different exposure to cybersecurity, even where the occupation involves handling personal information, using digital platforms or managing workplace risk. The problem is not only whether cyber units exist in training products, but whether secure digital behaviours are consistently taught, practised and assessed as part of occupational competence.

System-change recommendations

The recommendations below are designed as a connected reform sequence. Each recommendation addresses a specific system gap but depends on the others. National guidance without educator capability will not change delivery; practical infrastructure without curriculum alignment will remain peripheral; and pilots without evaluation and recurrent funding will not create system change.

Recommendation 1: Create a national coordination group for cybersecurity education and skills.

System issue addressed: Cybersecurity education is currently spread across schools, VET, universities, workforce policy and industry. These areas often work separately, which can lead to duplicated work, unclear responsibilities and gaps in learner pathways.

Proposed action: Establish a time-limited national coordination group to bring these areas together. The group should develop a shared national action plan for cybersecurity education, basic cyber capability and workforce pathways. Its role should not be to tell every provider how to teach cybersecurity. Instead, it should set common priorities, clarify who is responsible for what, identify gaps and dependencies, and report progress publicly.

Lead and supporting stakeholders: The Australian Government areas responsible for skills, education and national cybersecurity should lead this work in partnership with state and territory governments. Other stakeholders should include Jobs and Skills Australia, Jobs and Skills Councils, curriculum authorities, public and private providers, regulators, employers, professional bodies, educators and learner representatives.

Implementation and timeframe: In the first 6 months, agree on the group's purpose, membership, roles and decision-making process. Within 6 to 12 months, map current initiatives, identify gaps, clarify the difference between general cyber awareness and job-specific cyber capability, and publish a staged national action plan. Existing government and sector forums should be used where possible, rather than creating a permanent new body too early.

Enabling conditions and constraints: This work will need ministerial support, funding for coordination, transparent stakeholder selection and clear boundaries between coordination, regulation and training product development. Key risks include overlapping with existing bodies, consulting without real authority, and losing momentum after the first report.

Expected outputs and outcomes: The main outputs should include a national map of current initiatives and responsibilities, agreed priorities, shared terminology, and a public dashboard showing progress.

Potential indicators of success: Success could be measured by broad representation across sectors and jurisdictions, actions with named owners and timeframes, less duplicated work, and evidence that curriculum, funding and pathway decisions are guided by the shared national plan.

Recommendation 2: Define, map and pilot baseline cybersecurity capability across VET

System issue addressed: Cybersecurity awareness and occupational cyber risk are not treated consistently across ICT and non-ICT qualifications, even though cyber risk is now embedded in digitally enabled work across the economy.

Proposed action: Develop a clear baseline that explains what all VET learners should know and be able to do in relation to cybersecurity. This should include basic cyber awareness, safe digital behaviour

and workplace responsibilities. The baseline should then be adapted for different industries so learners understand the cyber risks relevant to their future jobs.

This should not automatically mean creating new units. Where cybersecurity is clearly relevant to occupational competence, it should be taught, practised and assessed as part of the qualification, rather than left only as an optional elective or general awareness activity. Depending on the qualification, this could be achieved through updated core units, revised assessment requirements, skill sets, companion resources, contextualised learning activities or practical workplace scenarios. Electives may still be appropriate where cyber capability is relevant to some roles within an industry but not required for all learners.

To test this approach, pilot cybersecurity-across-disciplines activities in three to five priority industries. These pilots could include examples such as protecting patient information in health, managing customer data in hospitality, securing connected equipment in manufacturing, or handling digital case records in community services. The purpose of the pilots would be to test what can realistically be embedded without overcrowding existing qualifications.

Lead and supporting stakeholders: Jobs and Skills Councils and national training product bodies should lead this work, supported by Jobs and Skills Australia, state and territory training authorities, employers, educators, cybersecurity specialists, industry regulators where relevant, and learner representatives. VET providers and industry partners should help co-design and test the pilots.

Implementation and timeframe: In the first 12 months, define the baseline and select three to five priority industries. In 12 to 24 months, design and deliver pilot activities with teaching resources and assessment examples. In 24 to 36 months, use the pilot findings to update training products, develop national resources and support wider implementation.

Enabling conditions and constraints: The baseline should be practical, vendor-neutral, easy to understand and aligned with existing digital capability and online safety work. Implementation will need educator support, employer input, funding and accessible resources. Key risks include curriculum overload, slow training product review timelines, uneven educator readiness and content becoming too generic.

Expected outputs and outcomes: This recommendation should produce a national VET cybersecurity baseline, sector-specific capability maps, tested learning activities, assessment examples, implementation guidance and evidence about where training product changes are needed.

Potential indicators of success: Success could be measured through the number of industries and qualifications mapped, the number of pilots completed, educator uptake, learner performance in practical cyber tasks, employer feedback, provider adoption and decisions made about scaling or updating training products.

Recommendation 3: Create a tiered national VET cybersecurity educator capability initiative

System issue addressed: Uneven educator confidence, limited industry currency opportunities and over-reliance on voluntary or one-off professional development.

Proposed action: Establish a tiered capability pathway for educators who teach specialist cybersecurity and for educators who need to embed foundational cyber practices in other disciplines. The pathway should combine foundation learning, practical laboratories, pedagogical support, industry externships, train-the-trainer development, mentoring and communities of practice.

Lead and supporting stakeholders: State and territory training authorities and major VET providers, coordinated nationally and delivered with universities, industry bodies, cybersecurity employers and professional associations. Providers remain responsible for workforce planning and release arrangements; industry partners contribute current practice and supervised placements.

Implementation and timeframe: In 0–6 months, define educator cohorts and capability outcomes. In 6–18 months, pilot blended programs with paid release time and regional access. Include short modules for broad participation and deeper pathways for specialist teachers. Evaluate practice change six and twelve months after completion. In 18–36 months, scale successful elements and develop formal recognition options, such as micro-credentials, digital badges, statements of attainment or credit toward relevant qualifications where appropriate.

Enabling conditions and constraints: Funding that covers educator time, not only course fees; access for sessional staff; mentor preparation; portable evidence of capability; and alignment with provider industry-currency processes. Risks include low participation due to workload, technical training disconnected from pedagogy, and inequitable access outside metropolitan areas.

Expected outputs and outcomes: A capability framework, funded professional learning pathways, industry placement agreements, shared resources and active communities of practice.

Potential indicators of success: Participation and completion by educator type and location; pre/post confidence and capability measures; number of industry placements; evidence of changed teaching practice; learner feedback; and retention of participating educators.

Recommendation 4: Develop shared practical cybersecurity learning environments

System issue addressed: VET providers do not have equal access to current cyber ranges, simulations, realistic scenarios, gamified learning resources and technical support. This can create uneven learning experiences for students, particularly in smaller, regional or less-resourced providers. Without shared practical environments, cybersecurity learning may remain too theoretical or dependent on the resources of individual providers.

Proposed action: Develop a shared-access model for practical cybersecurity learning environments, including cloud-based cyber ranges, safe simulation platforms, curated scenario libraries, Capture the Flag-style challenges and gamified learning activities. These environments should support specialist cybersecurity qualifications as well as contextualised cyber learning in other disciplines.

The resources should support different levels of learning, from foundational cyber awareness and safe digital behaviour through to more advanced technical problem-solving. Cyber ranges and simulations can support structured technical practice and assessment, while CTF-style challenges and gamified activities can strengthen learner engagement, confidence and practical application. Scenario libraries should include realistic workplace examples and be mapped to units of competency, with educator guidance to support consistent teaching and assessment.

Lead and supporting stakeholders: State and territory training authorities, public TAFEs, participating RTOs and industry partners should work together to develop and test the model, with national co-investment where shared infrastructure benefits more than one jurisdiction. Providers should lead assessment integration, while industry partners can support scenario validation, currency and mentoring.

Implementation and timeframe: In the first 12 months, review existing platforms, provider needs, regional access gaps and technical support requirements. In 12 to 24 months, pilot shared access with a small group

of providers and test a common support model. In 24 to 36 months, expand the model if it improves access, quality, educator confidence and learner outcomes.

Enabling conditions and constraints: Implementation will require sustainable licensing and support funding, educator onboarding, accessible design, vendor-neutral learning outcomes, quality scenario curation and clear governance for data, identity, platform security and vendor exit. Key risks include vendor lock-in, low utilisation, technical complexity, unclear maintenance responsibility, uneven educator readiness and resources that are engaging but not clearly linked to competency-based learning.

Expected outputs and outcomes: This recommendation should produce shared platform access, mapped practical scenarios, CTF-style challenges, gamified learning activities, educator support materials, utilisation data and more consistent access to safe cybersecurity practice environments.

Potential indicators of success: Success could be measured through the number and diversity of participating providers and learners, regional access, platform utilisation, completion of mapped practical tasks, educator satisfaction, learner confidence, cost per learner and evidence of improved practical cybersecurity capability.

Recommendation 5: Strengthen connected pathways and supported entry into cybersecurity work

System issue addressed: There are not always clear pathways between school, VET, higher education, industry certifications and cybersecurity employment. Many learners also have limited opportunities to gain practical experience, particularly because cybersecurity qualifications in Australia do not generally include mandatory industry placement requirements.

Proposed action: Develop clear regional and national pathway maps that show how learners can move from school into VET, higher education, certifications and cybersecurity employment. These pathways should include recognition of prior learning, credit transfer, articulation arrangements, mentoring, competitions, industry projects and supervised work-integrated learning opportunities.

International models such as AP Cybersecurity show that recognised school-level learning can create clearer pathways into VET and higher education. Australia could apply this principle by offering appropriate recognition, credit or articulation for substantial, quality-assured cybersecurity study.

A cyber clinic model could also be piloted in selected VET providers. In this model, advanced learners would work under educator and industry supervision to support eligible community organisations, not-for-profits or small businesses within a clearly defined service scope. Activities could include basic cyber awareness support, cyber hygiene checks, risk identification, use of approved assessment tools and preparation of practical recommendations. The model should not involve unsupervised technical intervention or high-risk security work.

Lead and supporting stakeholders: State and territory education and training departments, schools, VET providers, universities, employers, industry bodies and community organisations should work together on this recommendation. Jobs and Skills Australia and regional workforce bodies should provide evidence about workforce demand, emerging roles and transition barriers. Industry partners should support mentoring, supervision and validation of work-integrated learning activities.

Implementation and timeframe: In the first 12 months, map existing pathways and identify transition barriers in selected regions. In 12 to 24 months, develop articulation agreements, recognition arrangements, mentoring partnerships and learner-facing pathway information. During this period, selected providers could also design and trial a small cyber clinic pilot with clear supervision, risk, privacy and ethical protocols. In 24

to 36 months, evaluate learner outcomes, employer and community benefit, supervision requirements and employment transitions, then expand only the models that demonstrate clear value and manageable risk.

Enabling conditions and constraints: This will require coordination, employer support, learner career guidance, recognition of non-formal and prior learning, and strong safeguards for quality and safety. Any cyber clinic pilot would need a defined service scope, industry supervision, privacy and confidentiality arrangements, professional indemnity considerations, ethical protocols and clear limits on student responsibility. Key constraints include employer capacity, security and trust requirements, uneven regional demand, provider readiness and the need to protect participating organisations from risk.

Expected outputs and outcomes: This recommendation should produce pathway maps, recognition and articulation agreements, mentoring arrangements, cyber clinic pilot guidelines, clearer entry-level role descriptions and stronger links between VET learning and real-world cybersecurity practice.

Potential indicators of success: Success could be measured through school-to-VET and VET-to-higher-education transitions, recognition or credit granted, participation in mentoring, competitions, industry projects or cyber clinic activities, learner confidence and performance, community or employer feedback, course completion, employment outcomes and learner perceptions of pathway clarity.

Taken together, these recommendations provide a connected reform pathway for strengthening cybersecurity education across the Australian VET system. Their impact will depend not only on policy coordination, curriculum alignment, educator capability, practical infrastructure and learner pathways, but also on how they are implemented, funded and evaluated. Equity, inclusion and regional access must be built into each initiative so that learners and educators are not disadvantaged by location, disability, gender, cultural background, provider resources or prior digital experience. Successful pilots and shared initiatives must also have a clear pathway to sustainable funding and institutional ownership, including provision for educator release time, technical support, platform maintenance, evaluation and governance. Progress should be measured through a simple impact framework that looks beyond activity counts, such as workshops delivered or resources developed, and considers whether educator practice changes, learners develop practical capability, pathways improve, access becomes more equitable and successful initiatives are adapted, scaled or embedded. Without these conditions, cybersecurity education reform risks remaining dependent on short-term projects, local champions and uneven provider capacity rather than becoming an embedded and enduring part of Australia’s VET system.

Future Directions for the Fellow

The Fellowship has identified several areas for future exploration, implementation and sector contribution. The Fellow intends to continue supporting conversations on cross-disciplinary cybersecurity education, educator capability development, practical learning environments and stronger pathways between education and work within the Australian VET sector.

Future work may include developing professional learning workshops for VET educators, contributing to cross-disciplinary curriculum pilots, supporting industry-informed teaching resources, and exploring practical learning activities such as cybersecurity clubs, Capture the Flag-style challenges, gamified learning and scenario-based assessments. These initiatives would aim to help educators embed cyber awareness, safe digital behaviour and occupational cyber risk into both specialist and non-specialist vocational disciplines.

The Fellow also intends to continue sharing Fellowship findings through conferences, sector forums, professional networks and collaborative projects with education, industry and government stakeholders. This will support broader discussion about how cybersecurity capability can be embedded more consistently across VET, while maintaining flexibility for different industries, learner groups and provider contexts.

Considerations and Limitations

The Fellowship provides transferable insights rather than a direct implementation model for Australia. International examples must be adapted to Australia's federated education system, competency-based VET model, training product arrangements, funding settings and diverse provider landscape.

The findings should also be understood in the context of a rapidly changing cybersecurity environment. Technologies, threats, workforce needs and teaching resources will continue to evolve, so any implementation should include ongoing review, sector consultation and evidence-informed adjustment over time.

07
Impacts of Fellowship

The Fellowship has generated impacts at personal, professional, organisational and broader sector levels. Some outcomes have already occurred, including increased professional confidence, expanded national and international networks, changes in classroom delivery, greater student participation in practical cybersecurity activities and emerging internal knowledge sharing at Victoria University. Other impacts remain at an early stage, including educator capability activities, sector collaboration and pilot initiatives. At the time of publication, no formal organisational or sector-wide policy change had been confirmed as a direct result of the Fellowship. However, the Fellowship has established a strong foundation for continued dissemination, collaboration and future implementation.

Personal Impact

The Fellow is deeply grateful for the trust placed in him by the International Specialised Skills Institute and the Victorian Skills Authority to undertake this Fellowship. The opportunity enabled him to investigate international approaches to cybersecurity education and engage with leading educators, researchers, policymakers and industry representatives across several countries.

One of the most significant personal outcomes has been increased confidence. Through meetings with internationally recognised leaders in cybersecurity education, workforce development and policy, the Fellow became more confident in engaging with senior stakeholders and contributing to national and international discussions. The Fellowship also strengthened his ability to critically examine education systems, identify opportunities for improvement and advocate for change within the Australian context.

The Fellowship further increased the Fellow's confidence in public speaking and knowledge sharing. Before the Fellowship, he had fewer opportunities to present to large and influential audiences. Since undertaking the research, he has presented emerging findings at conferences, working groups and professional forums. These experiences have strengthened his confidence in communicating complex ideas and contributing to discussions about cybersecurity education, workforce development and the future of vocational learning.

On a broader personal level, the Fellowship expanded the Fellow's understanding of what can be achieved through international collaboration. Managing the research, international engagement, travel, stakeholder meetings, report development and dissemination activities also strengthened his resilience, adaptability and motivation. The experience reinforced his sense of purpose as an educator and his commitment to improving cybersecurity education for learners, educators and the wider community.

Professional Practice and Leadership Impact

The Fellowship has had a direct impact on the Fellow's professional practice as a vocational education teacher and emerging researcher. Engagement with international experts provided new perspectives on educator capability, practical learning, curriculum integration, workforce development and education-to-employment pathways.

A major professional impact has been a stronger emphasis on hands-on and experiential learning. International examples involving cyber ranges, cyber clinics, simulations, competitions and challenge-based learning reinforced the importance of allowing learners to apply knowledge in realistic settings. As a result, the Fellow has increased the use of practical activities, real-world cybersecurity scenarios and contemporary examples within classroom delivery.

During the Fellowship period, the Fellow designed and delivered two diploma-level cybersecurity courses: Ethical Hacking and Incident Detection and Response. These courses were not developed solely as a direct result of the Fellowship; however, the international learning strengthened the Fellow's emphasis on practical delivery, current industry context and authentic cybersecurity scenarios. Students have responded positively to the hands-on content and to the inclusion of emerging cybersecurity trends and current information drawn from the Fellow's ongoing engagement with NCyTE and EU CyberNet.

The Fellowship also provided continuing access to current international knowledge. Through monthly EU CyberNet expert meetings and engagement with NCyTE, the Fellow has remained informed about emerging cyber threats, threat actors, geopolitical developments, workforce issues and changes in cybersecurity practice. This has enabled him to introduce more current examples and industry-relevant discussion into teaching, helping learners connect technical concepts with the evolving cybersecurity environment.

Another important professional outcome has been the increased use of competitions and challenge-based learning. The Fellow introduced students to cybersecurity competitions and encouraged participation in Cyber Battle Australia 2026, which involved more than 300 participants from across Australia. Two of the Fellow's students progressed to the Grand Final, with one student securing a Top 3 finish nationally, while the Fellow won first place in the Sponsors League. While this single outcome does not demonstrate broad student impact, it provides a strong example of how competition-based learning can increase engagement, practical capability and awareness of cybersecurity career pathways.

Figure 15. Fellow with John Burgess and VU Students at Cyber Battle 2026

The Fellowship has also strengthened the Fellow's research and leadership capability. Direct access to international models and expert perspectives has improved his ability to compare education systems, assess the transferability of overseas initiatives and identify realistic adaptations for Australian VET. This has increased his capacity to contribute to curriculum discussions, applied research, professional learning and broader sector conversations.

The Fellowship also produced significant professional-network outcomes. Nationally, the Fellow established relationships with education and cybersecurity stakeholders through professional groups and sector networks. Internationally, the Fellow established relationships with organisations and experts associated with NIST, NCyTE, Rogers Cybersecure Catalyst, Tallinn University, the Estonian Information System Authority and EU CyberNet. A particularly significant outcome was his acceptance into the EU CyberNet Expert Pool. He was also invited to participate in the California Cybersecurity Task Force Workforce Development and Education Subcommittee. These appointments have expanded his professional network and created opportunities to contribute to international discussions on cybersecurity education, workforce development and policy.

Organisational Impact at Victoria University

The Fellowship has begun to generate organisational impact at Victoria University through changes in teaching practice, internal knowledge sharing and the development of new practical learning opportunities for students. The international findings have strengthened the use of practical exercises, contemporary examples and real-world scenarios in the delivery of Ethical Hacking and Incident Detection and Response. These changes represent confirmed practice-level impacts within the Fellow's teaching responsibilities.

The Fellowship has also created opportunities to share knowledge more broadly across the University. The Fellow has discussed with his manager the possibility of presenting Fellowship findings at Victoria University's annual Teaching and Learning Conference. This would provide an internal platform to share international approaches to educator capability, practical cybersecurity learning, curriculum integration and workforce preparation with a wider group of teaching staff.

Internal engagement has also occurred through VUCyber, which supported the promotion of the Fellow's cybersecurity workshop at the Illuminate Forum 2026 across the University. As a result, Victoria University staff attended the session and were exposed to the Fellowship findings and practical approaches to cybersecurity education. This represents an early organisational impact by extending the reach of the research beyond the Fellow's immediate teaching area and encouraging internal discussion about cybersecurity capability and education.

The Fellowship's emphasis on practical and challenge based learning has also contributed to the development of a new opportunity for Victoria University students. Through continued engagement with Australian cybersecurity initiatives, the Fellow established initial contact with Security Impossible, an Australian cyber range provider. Security Impossible has agreed to conduct a Capture the Flag (CTF) cybersecurity challenge for Victoria University students later in 2026 at no cost. This will provide students with an additional industry-linked opportunity to apply cybersecurity knowledge and develop practical skills in a challenge-based environment.

At the time of publication, no formal university-wide policy or teaching methodology change had been introduced as a direct result of the Fellowship. However, changes within the Fellow's teaching practice, engagement through VUCyber, staff participation in the Illuminate Forum workshop, discussions regarding the Teaching and Learning Conference, and the planned CTF initiative demonstrate growing organisational

impact and provide a foundation for further knowledge sharing, practical learning and industry collaboration across Victoria University.

Broader K–12 and VET Sector Impact

The broader impact of the Fellowship remains at an early stage, but several important connections have been established. The Fellowship has contributed to emerging discussions about positioning cybersecurity not only as a specialist technical field, but also as a foundational capability relevant across education, training and digitally enabled occupations

The Fellowship findings have generated interest among educators and sector stakeholders in areas such as cybersecurity across disciplines, educator capability, practical learning, cyber awareness and workforce pathways. Following one national education presentation, several educators contacted the Fellow to request links to international curriculum and teaching resources. This represents an early example of dissemination progressing into continued professional engagement, although there is not yet evidence that the resources have been formally adopted by other organisations.

The Fellow has also developed relationships with representatives from Departments of Education across several Australian states and territories through the CyberMarvel Cyber Awareness Working Group. These relationships have created opportunities to exchange ideas and share international examples relating to age-appropriate cyber awareness, digital safety and cybersecurity education. At the time of publication, no formal curriculum or policy change had been confirmed as a result of this engagement.

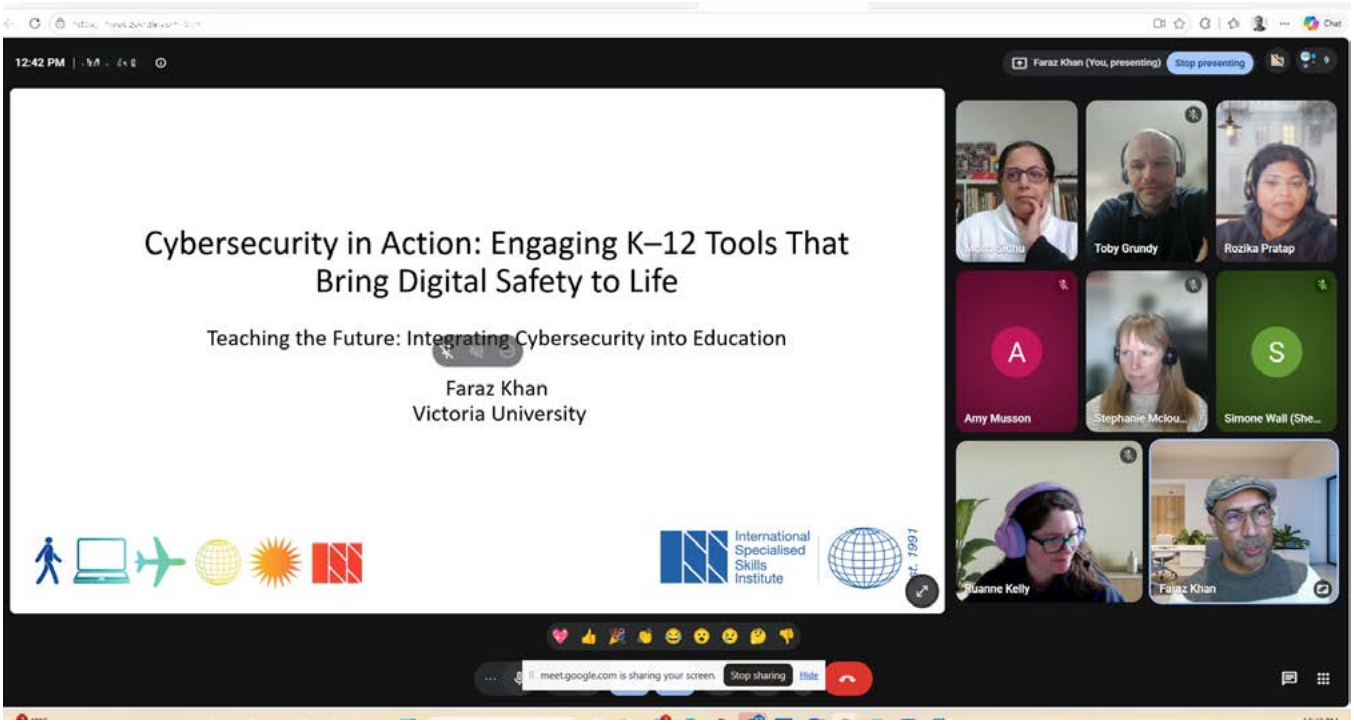


Figure 16. Faraz Khan presenting to CyberMarvel Cyber Awareness Working Group

The Fellowship has also created potential future engagement channels with organisations and initiatives concerned with education, workforce development and training. These may provide opportunities to share findings relating to cybersecurity pathways, training products, cross-disciplinary capability, practical learning

and industry engagement. However, these relationships remain at an early stage and should not yet be presented as demonstrated sector impact.

Potential future impacts include educator capability workshops, cross-disciplinary cybersecurity pilots, shared practical learning resources, stronger industry partnerships and supervised work-integrated learning models. These opportunities require further stakeholder consultation, identified partners, organisational ownership, funding and evaluation before they can progress into formal implementation.

The clearest sector impact to date is therefore increased awareness, professional engagement and the creation of new relationships through which the findings may influence future practice. No formal state or sector-wide policy, curriculum or methodology change had occurred at the time of publication.

Overall, the Fellowship has strengthened the Fellow’s confidence, teaching practice, professional standing and international networks. It has also generated emerging organisational interest and early sector engagement. Broader and longer-term impact will depend on continued collaboration, stakeholder commitment, practical implementation and evidence that the findings lead to sustained improvements for educators, learners, providers and industry.

The dissemination activities and stakeholder-engagement channels supporting these emerging impacts are outlined in Section 8.

08

Sector Engagement (Dissemination)

The Fellow recognises that the value of the Fellowship depends on effectively communicating its findings and creating opportunities for continued dialogue, collaboration and implementation. This section focuses on the channels, audiences and engagement strategies used to disseminate the research. The personal, professional, organisational and broader sector impacts arising from these activities are discussed in Section 7.

Dissemination has involved national conferences, professional forums, working groups, professional publications, internal university networks and direct resource sharing. The Fellow has sought to tailor key messages to different audiences. Engagement with educators has focused on practical teaching resources, educator capability and curriculum approaches. Discussions with policymakers and system leaders have emphasised governance, implementation and workforce capability, while engagement with industry stakeholders has focused on practical learning, industry currency and education-to-employment pathways.

Completed Dissemination Activities

The Fellow has disseminated Fellowship findings through national conferences, professional forums and industry publications, including the AVETRA Conference 2026, EDUtech Australia 2026, the Illuminate Forum 2026 and Australian Cyber Security Magazine. These activities have enabled the Fellow to engage with educators, researchers, industry representatives, government stakeholders and sector leaders.

At the AVETRA Conference 2026, the Fellow presented international findings relating to the integration of cybersecurity capability across vocational disciplines. The presentation focused on the growing relevance of cyber risk beyond specialist ICT qualifications and the need to consider cybersecurity within digitally enabled occupations.

At EDUtech Australia 2026, the Fellow shared international examples of cybersecurity education, digital safety, teacher resources and game-based learning. Following the presentation, several educators contacted the Fellow to request links to curriculum materials and teaching resources discussed during the session. The Fellow responded by sharing relevant resources and maintaining contact where further information was requested.

Figure 17. Faraz Khan presenting at AVETRA 2026 Conference

Figure 18. Faraz Khan presenting at EDUtech AU 2026 Conference

The Fellow also delivered a cybersecurity workshop at the Illuminate Forum 2026. VUCyber supported the internal promotion of the workshop across Victoria University, helping extend awareness of the session to university staff. The workshop provided an opportunity to share practical approaches to cybersecurity education and encourage discussion among educators and sector participants.

Figure 19. Faraz Khan presenting at ILLUMNATE Forum 2026 at VDC

Dissemination has also extended through professional publication. In July 2026, the Fellow's article, "Cybersecurity Across Disciplines: Why Every Profession Needs Cyber Capability," was published in Australian Cyber Security Magazine (Khan, 2026). Drawing on findings from the Fellowship, the article highlighted the need to move beyond viewing cybersecurity solely as an ICT specialisation and consider foundational and occupation-specific cyber capability across digitally enabled professions. The publication provided an opportunity to communicate key Fellowship findings and recommendations to a broader cybersecurity, industry and workforce audience.

The Fellow has also shared international K–12 findings through participation in the CyberMarvel Cyber Awareness Working Group. This forum has enabled engagement with representatives from Departments of Education across several Australian states and territories. Information shared through the group has included international approaches to cyber awareness, digital safety, age-appropriate curriculum resources and game-based learning.

Planned Dissemination

Further dissemination is planned during late 2026 and 2027. The Fellow is confirmed to present at CyberCon 2026, providing an opportunity to communicate the Fellowship findings to cybersecurity professionals, industry representatives, government stakeholders and educators.

There is also a potential opportunity to share the Fellowship findings through Victoria University's annual Teaching and Learning Conference. This proposed presentation would provide an internal channel for sharing international approaches to educator capability, practical learning, curriculum integration and workforce preparation with a broader group of teaching staff.

Other proposed activities may include presentations to education, VET and industry groups, educator capability workshops, stakeholder briefings and meetings, participation in relevant working groups and consultation processes, and the continued sharing of international teaching and curriculum resources. Initial connections have also been established with AISA's Cyber Australia magazine and AVETRA's Research Today magazine to explore opportunities for publishing articles based on the Fellowship findings.

Policy, Industry and System-Level Engagement

The Fellow intends to use the Fellowship findings to contribute to policy, workforce and system-level discussions. Engagement will focus on translating the international evidence into concise and relevant messages for Australian stakeholders rather than seeking to directly reproduce overseas models.

Through CyberMarvel, the Fellow has already established a channel for engaging with representatives from state and territory Departments of Education. The Fellow intends to continue using this network to share relevant findings and participate in discussions about cyber awareness, digital safety, teacher capability and cybersecurity education in schools.

The Fellow has also registered his interest with the Australian Computer Society's CyberPath project and Commonwealth Scientific and Industrial Research Organisation (CSIRO) Education and Outreach. Engagement with the Future Skills Organisation has progressed further, with the Fellow participating in an initial meeting following an opportunity provided by Patrick Kidd OBE OAM, CEO of the Future Skills Organisation. This connection has enabled the Fellow to engage with the Future Skills Organisation's ICT Training Package project and contribute to discussions relevant to the future development of cybersecurity and digital skills within Australia's vocational education and training sector.

Engagement with the Australian Computer Society and CSIRO remains at an early stage and represents potential future engagement channels rather than formal collaborations. The Fellow intends to continue seeking opportunities to share relevant Fellowship findings with these organisations, particularly in relation to cybersecurity pathways, workforce capability, training products, curriculum integration and industry engagement.

No formal policy or industry-guideline change had occurred as a direct result of the Fellowship at the time of publication. Current engagement is therefore focused on sharing evidence, building relationships and contributing to discussions that may inform future policy, curriculum and workforce initiatives.

The Fellow views dissemination as an ongoing process rather than a series of isolated presentations. Continued communication and follow-up will be important to move from awareness raising to collaboration and possible implementation. Through continued dissemination, stakeholder engagement and collaboration, the Fellow aims to support informed discussion about the challenges and opportunities facing cybersecurity education. The longer-term goal is to contribute to sustainable improvements in educator capability, curriculum relevance, workforce readiness and cybersecurity awareness across Australian K–12 and VET education.

09 Conclusion

This Fellowship examined how cybersecurity education, digital safety and workforce development can be strengthened across the education pipeline, with particular relevance to Australian and Victorian VET. Its central finding is that Australia's principal challenge is not the absence of qualifications, teaching resources, awareness campaigns, professional learning or industry initiatives. The more significant problem is that these activities are not consistently connected through shared policy direction, sustainable funding, clear governance, responsive curriculum arrangements, educator capability, practical infrastructure, learner pathways and meaningful evaluation. As cyber risk becomes embedded in almost every digitally enabled occupation, this fragmentation limits the capacity of the education and training system to prepare learners, support educators and respond coherently to changing workforce needs.

The Australian consultation and international research point to the same underlying conclusion: effective cybersecurity education depends on a system of mutually reinforcing elements rather than a collection of isolated programs. Australian VET educators reported barriers involving confidence, time, access to current resources, practical learning environments, professional development and industry engagement. The international examples demonstrated that these barriers can be reduced when educator development is structured, funded, practical and sustained; when curriculum expectations are supported by implementation guidance; and when providers can access shared resources, technical platforms and professional networks. The evidence therefore indicates that educator capability should be treated as core workforce infrastructure, not as an optional responsibility left to individual teachers or providers.

The North American findings showed the value of common workforce frameworks, coordinated resource development, industry-supported educator programs, shared cyber ranges, practical competitions, supervised service-based learning and clearer education-to-employment pathways. These examples also revealed the limits of decentralised and grant-dependent activity when successful programs lack continuation funding, institutional ownership or equitable access. Estonia demonstrated a different but complementary lesson. Its strength lies not in a single cybersecurity subject or initiative, but in the alignment of digital competence expectations, teacher development, specialist implementation support, organisational cyber responsibilities, continuous awareness and experiential learning. Collectively, these international examples suggest that cybersecurity education becomes more effective when national direction, local implementation, educator support, practical learning and workforce pathways operate as a connected ecosystem.

For Australia, this does not mean importing a single overseas framework, curriculum, cyber range or teacher-development model. The United States, Canada and Estonia operate within different governance, funding and curriculum environments, while Australian VET is shaped by federal arrangements, national training products, state and territory responsibilities, provider diversity and competency-based assessment.

International approaches must therefore be adapted to Australian conditions. The most transferable principle is the need for a shared architecture that establishes clear expectations and responsibilities while allowing delivery to be contextualised for different industries, qualifications, learner groups and provider settings.

A central implication is that cybersecurity can no longer be confined to specialist ICT programs. All learners require a baseline of cyber awareness, cyber hygiene, safe digital behaviour and workplace responsibility, while particular occupations require additional practices reflecting their specific risks. Health, community services, business, manufacturing, hospitality and other digitally enabled sectors handle information, systems and technologies in different ways; their cybersecurity learning should therefore be relevant to workplace decisions rather than reduced to generic awareness content. Defining and testing a cross-disciplinary VET baseline would provide a clearer foundation for determining where cyber capability should be embedded in core requirements, assessment, skill sets, electives, companion resources or contextualised learning activities.

The report's recommendations respond to these weaknesses as a connected reform sequence. A national coordination group would establish shared direction, clarify responsibilities and reduce duplication. A baseline cybersecurity capability across VET would connect general safe practice with sector-specific occupational requirements. A tiered educator capability initiative would support both specialist cybersecurity teachers and educators embedding cyber practices in other disciplines through practical learning, pedagogical support, mentoring, industry externships and formal recognition where appropriate. Shared practical learning environments would improve equitable access to cyber ranges, simulations, scenario libraries, Capture the Flag challenges and gamified activities. Stronger articulation, recognition, mentoring, industry projects, supervised work-integrated learning and carefully governed cyber clinic pilots would help learners translate education into experience and employment.

Several actions can begin in the short term. Governments and sector bodies can map existing initiatives, identify gaps and responsibilities, agree on shared terminology, define educator cohorts and capability outcomes, review available practical platforms, identify priority industries for cross-disciplinary pilots and map current learner pathways. Providers can expand scenario-based teaching, support educator communities of practice, strengthen industry engagement and use existing competitions, simulations and resources more strategically. These actions would create evidence, build relationships and test implementation without waiting for complete structural reform.

Longer-term change will require more than additional projects. Within a staged implementation period, pilot findings must inform training product development, assessment guidance, educator recognition, articulation arrangements, shared infrastructure and workforce planning. Programs that demonstrate value will need pathways to recurrent funding and institutional ownership, including provision for educator release time, platform maintenance, technical support, mentoring, governance and evaluation. Progress should be judged not only by participation, resource downloads or events delivered, but by whether educator practice changes, learners demonstrate practical capability, access becomes more equitable, pathways become clearer and employers observe stronger workforce readiness.

The implications extend across the system. Policymakers must connect cybersecurity, education and workforce priorities rather than treating them as separate policy domains. Schools can build early awareness, confidence and interest through age-appropriate, progressive and experiential learning. VET providers can translate foundational capability into occupational practice and provide accessible entry and progression pathways. Educators require time, current knowledge, practical experience and sustained support to deliver this work effectively. Industry must contribute more than endorsements by helping validate curriculum, provide mentors, offer supervised experiences and clarify realistic entry-level expectations.

Professional bodies, universities and government agencies can support shared resources, research, recognition and evaluation.

For Victoria, the Fellowship identifies an opportunity to demonstrate national leadership through carefully designed pilots in educator capability, cross-disciplinary curriculum integration, shared practical environments and supported pathways into work. Such pilots should be inclusive, accessible to regional and sessional educators, aligned with national arrangements and designed from the outset for evaluation and possible scaling. Victoria's VET system is well placed to show how specialist cybersecurity expertise can be connected with broader workforce capability across multiple industries.

The Fellowship does not suggest that education alone can eliminate cyber risk or resolve every workforce shortage. It does, however, show that education and training are essential components of national cyber resilience and that their contribution will remain limited while activity is fragmented, optional or dependent on individual champions. Sustained improvement requires a shift from isolated initiatives to coordinated capability building across curriculum, educators, providers, workplaces and learner pathways. Australia will not build enduring cyber resilience through one-off programs alone; it will build it by making secure digital practice an expected, supported and continuously strengthened part of how every learner is prepared for work and participation in a digital society.

10 References

ACS - Cybersecurity micro-credential. (2025). Acs.org.au. https://www.acs.org.au/ict-educators/cybersecurity-micro-credential.html

AP Cybersecurity – AP Central | College Board. (2025). Collegeboard.org. https://apcentral.collegeboard.org/courses/ap-cybersecurity

ARC Project – Teach Cyber. (2026). Teachcyber.org. https://teachcyber.org/arc/

Australian Government. (2023). 2023-2030 Australian Cyber Security Strategy. Australian Government. https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Bishop, M., Cerrone, B., Dai, J., Dark, M., Daugherty, J., Huff, P., Tang, C., & Tucker, C. (2025). Supplement to CSEC 2017: Foundational Cybersecurity Content and Instructional Guidance for Secondary and Postsecondary Cybersecurity Education. https://doi.org/10.1145/3715982

Canada, E. (2025). Introduction to cyber security for educators - Canadian Centre for Cyber Security. Canadian Centre for Cyber Security. https://www.cyber.gc.ca/en/education-community/learning-hub/courses/introduction-cyber-security-educators

Catalyst Cyber Clinic. (2025, July 11). Rogers Cybersecure Catalyst. https://cybersecurecatalyst.ca/clinic/

Catalyst Fellowship Program. (2026, May). Rogers Cybersecure Catalyst. https://cybersecurecatalyst.ca/fellowship-program/

Center to Advance CTE. (n.d.). RING (Relationships, Interests, Needs, and Growth). https://caeepnc.org/ring/

CLARK | Cybersecurity Library. (2024). Clark.center. https://clark.center/

CSER Group. (n.d.). Available MOOCs. The University of Adelaide. https://csermoocs.adelaide.edu.au/available-moocs

CSET. (2020). Hsdl.org. https://www.hsdl.org/c/view?docid=695539

CyAD Summit: Cybersecurity Across Disciplines | NCyTE Center. (2022). Ncyte.net. https://www.ncyte.net/resources/events/cyad-summit-cybersecurity-across-disciplines

Cyber Challenge. (2026, May 14). Rogers Cybersecure Catalyst. https://cybersecurecatalyst.ca/cyber-challenge/

Cyber Florida. (n.d.). Innovative virtual cyber program for Florida public schools. https://cyberflorida.org/innovative-virtual-cyber-program-for-florida-public-schools/

Cyber test. (2023). RIA. https://www.ria.ee/en/cyber-security/cyberspace-analysis-and-prevention/kubertest

CyberSpike. (2026). CyberSpike. Google Docs. https://docs.google.com/presentation/d/15d-OGUUNe5IbuBkT_agiVBkT0fHI-F4wa-LE_xAWLeU/present?slide=id.p1

CyberSupply. (2023). Cybersupply.org. https://cybersupply.org/

Decrypt. (2026). Vt.edu. https://decrypt.cyberrange.vt.edu/

DigCompEdu. (n.d.). Joint-Research-Centre.ec.europa.eu. https://joint-research-centre.ec.europa.eu/digcompedu_en

Digital Competence: Empowering teachers and students - Estonia. (n.d.). Education Estonia. https://www.educationestonia.org/innovation/digital-competence/

Digital Competence: Empowering teachers and students - Estonia. (n.d.). Education Estonia. https://www.educationestonia.org/innovation/digital-competence/

Education Estonia. (n.d.). How it all began? From Tiger Leap to digital society. Education Estonia. https://www.educationestonia.org/tiger-leap/

Education, D. of. (2022, June 23). Cybermarvel | NSW Government. Www.nsw.gov.au. https://www.nsw.gov.au/education-and-training/cybermarvel

Estonian information security standard (E-ITS). (2022). RIA. https://www.ria.ee/en/cyber-security/management-state-information-security-measures

Khan, F. (2026, July 16). Cybersecurity across disciplines: Why every profession needs cyber capability. Australian Cyber Security Magazine. https://australiancybersecuritymagazine.com.au/cybersecurity-across-disciplines-why-every-profession-needs-cyber-capability/

Hackersjack. (2022). Hackersjack.com. https://hackersjack.com/

Kerli Kuusk. (2023, November 10). Õppematerjalid “Targalt internetis ABC minu koolis” nüüd avalikud - Targalt Internetis. Targalt Internetis. https://www.targaltinternetis.ee/uudised/2023/11/oppematerjalid-targalt-internetis-abc-minu-koolis-nuud-avalikud-2/

National Cybersecurity Training and Education Center. (n.d.). Faculty fellowship program. NCyTE. https://www.ncyte.net/industry/industry-resources/faculty-fellowship-program

National Initiative for Cybersecurity Careers and Studies. (2025, May 29). NICE Workforce Framework for Cybersecurity (NICE Framework). National Initiative for Cybersecurity Careers and Studies. https://niccs.cisa.gov/tools/nice-framework

NCyTE Center. (2022). Ncyte.net. https://www.ncyte.net/

Pozogina, K. (2023, June 8). Digital education in Estonia [Conference presentation]. Digital Education Conference, Cyprus. https://www.pi.ac.cy/pi/files/texnologia/imerides/digitaleducpi2023/presentation_Kerli_Pozogina_20230608.pdf

Rogers Cybersecure Catalyst. (n.d.). Cybersecurity for K–12 educators. Toronto Metropolitan University. https://cybersecurecatalyst.ca/cybersecurity-for-k-12-educators/

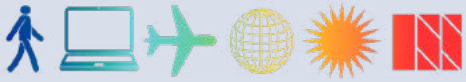
Security Awareness Curriculum - Future Innovators | Fortinet. (2025). Fortinet. https://www.fortinet.com/training/security-awareness-training/future-innovators

Security Impossible. (n.d.). Australia's cyber range for education. https://www.securityimpossible.com/

SuperCyberKids – Erasmus+ Programme. (2026). Supercyberkids.eu. https://www.supercyberkids.eu/

U.S. Cyber Range. (n.d.). Uscyberrange.org. https://www.uscyberrange.org/

Virginia Cyber Range. (n.d.). Www.virginiacyberrange.org. https://www.virginiacyberrange.org/



International
Specialised
Skills
Institute

est. 1991