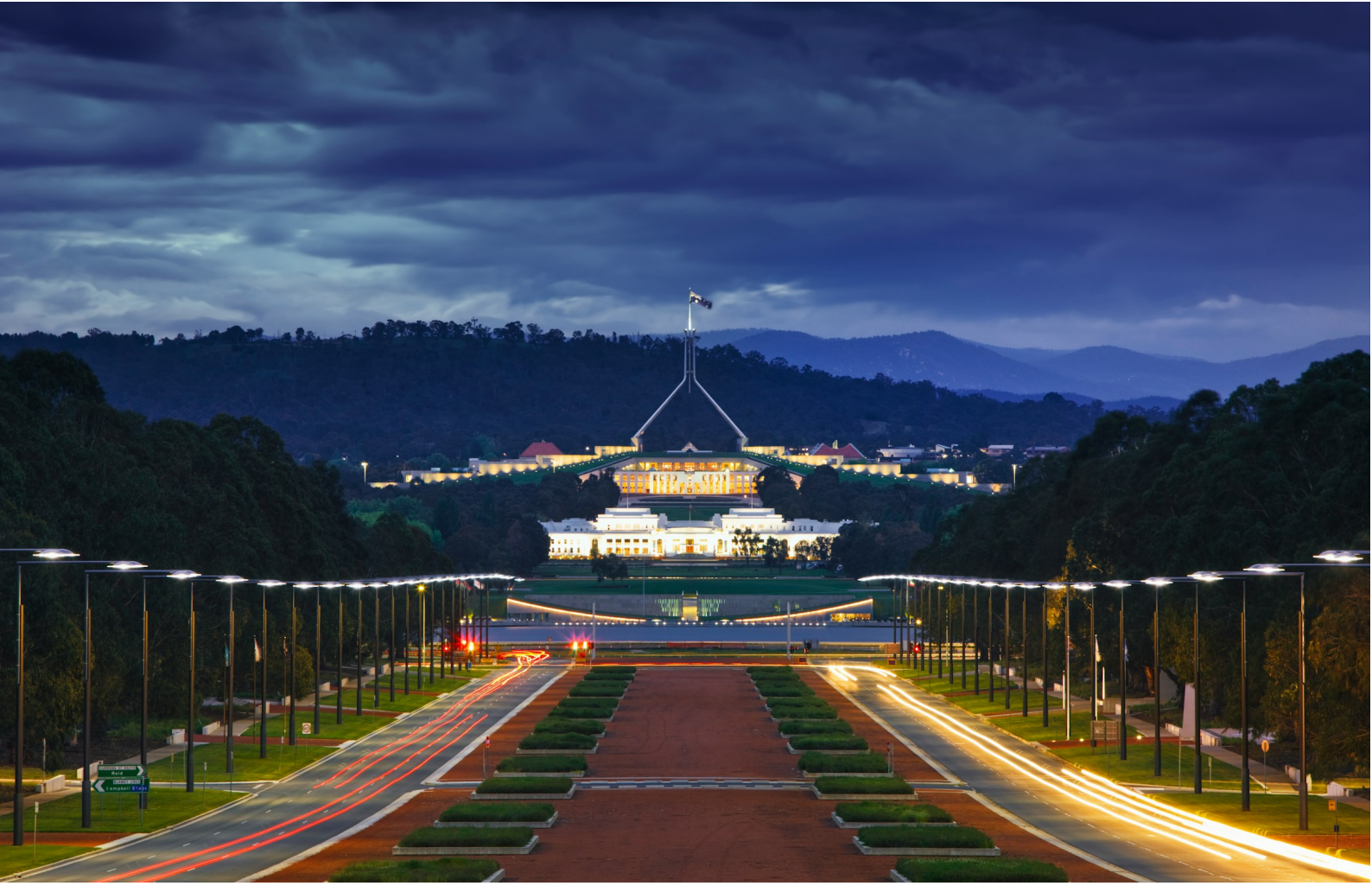


CYBER SECURITY EDUCATION ENGAGEMENT IN AUSTRALIA

17–19 MARCH, 2025 | CANBERRA

An International Cybersecurity Education Collaborative (ICEC) initiative, supported by:

NCYTE CENTER
National Cybersecurity Training & Education Center

CSE CONNECT

ACKNOWLEDGEMENT AND THANKS

NCyTE, CSE Connect and members of the delegations would like to acknowledge and thank Prof. Glenn Withers and Adam Henry at the Social Cyber Institute for their exceptional development and coordination of the programme. They also acknowledge and appreciate the time, effort and hospitality dedicated by their Australian hosts throughout their meetings and participation.

ABOUT NCYTE, CSE CONNECT AND ICEC

NCyTE Mission: The National Cybersecurity Training & Education (NCyTE) Center advances cybersecurity education in the U.S. by investing in technological innovation, resources, professional development and tools to support faculty, community colleges, and the workforce pipeline of tomorrow.

CSE Connect: A national cyber security education network, our mission is to promote innovative and impactful cyber security education practice across the UK academic landscape. We network Government, Industry and Academia collaborators, to inspire current and future generations of cyber security professionals. CSE Connect is sponsored by the National Cyber Security Centre (NCSC).

ICEC: The International Cybersecurity Education Collaborative (ICEC) is based on a collaborative network established between UK and US cyber security educators, in partnership with the US federally funded, National Cybersecurity Training and Education Center (NCyTE). This exciting programme aims to build further collaboration, as described in the Conclusions.

Cover photograph: Photo by Social Estate on Unsplash

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This report provides a summary and analysis of the International Cybersecurity Education Collaborative (ICEC) supported visit to Canberra, Australia, which took place from 17–19 March 2025.

It details the interaction and outcomes of this collaborative effort between cyber security education experts, policymakers, and industry leaders from the UK, US, and Australia. The initiative aimed to address critical cyber workforce challenges and share innovative strategies for education and skills development. The dialogue presented an opportunity for reciprocal fact-finding, knowledge sharing and engagement with Australian government, industry, and education figures. It aimed to create the foundations for building long-term partnerships.

The initiative focused on thought leadership and collaboration to solve shared education and workforce challenges. Discussions throughout the visit highlighted the thriving cyber sector in Canberra and impressive relationships between business, government, and academia. It illustrated innovative hands-on education initiatives but also challenges in standardising work roles and tasks, the complexity of professionalising cyber security, and structural issues affecting the skills pipeline and workforce management.

Key takeaways included the value of cyber ecosystem approaches, diversity initiatives, industry engagement in education, and the need for flexible and data-driven approaches to skills development. The visit was perceived as very successful, with early output looking promising and longer-term collaboration highly likely.

The report proposes ten recommendations, summarised as:

1. Develop an Australian national community for cyber security education collaboration.
2. Develop models for cyber security ecosystems that take account of the dynamics of national coordination/standardisation and regional innovation/autonomy.
3. Collaborate on models and best practices for enhancing industry-education engagement.
4. Collaborate on refining workforce language and frameworks.
5. Continue development of security mindset and tradecraft training.
6. Support faculty development.
7. Collaborate on developing integrated communities, potentially mirroring or linking existing models like the US CAE and UK ACE community.

8. Share insights and develop joint approaches to address structural changes needed in the education and workforce management landscape, such as creating more early-stage career routes.
9. Explore Data-Driven Approaches.
10. Utilise existing structures like ICEC for ongoing information exchange, bilateral discussions, and joint working initiatives.

It is intended to hold a number of events in the UK, US and online over the summer of 2025, aimed at providing opportunities to advance this work and take forward the recommendations.

INTRODUCTION, CONTEXT AND PURPOSE

This report provides a summary and analysis of the Cyber Security Education Collaborative (ICEC) supported visit to Canberra, Australia, which took place from 17–19 March 2025. It outlines the purpose, format, key meetings, discussions, and outcomes of this collaborative effort between cyber security education experts, policymakers, and industry leaders from the UK, US, and Australia. The initiative aimed to address critical cyber workforce challenges and share innovative strategies for education and skills development.

Originally planned as a large in-person delegation, US funding constraints led to a reconfigured format combining a small in-person delegation with significant on-line participation. The visit provided an important opportunity for reciprocal fact-finding, knowledge sharing, engagement with Australian government, industry, and education figures, and building long-term partnerships.

This engagement in Australia was an ICEC (International Cybersecurity Education Collaborative (ICEC), initiative. Its core aim was to foster international collaboration with Australian stakeholders to tackle critical cyber workforce challenges and exchange innovative strategies for education and skills development. This brought together experts, policymakers, and industry leaders from the UK and US to engage with their Australian counterparts. The initiative was set within the broader context of enhancing global cyber resilience and education best-practice, building on several existing highly successful UK-US relationships in this field.

The initiative was explicitly designed as a platform for thought leadership, allowing participants to share expertise across the three countries. It aimed to foster collaboration to develop solutions to shared cyber workforce challenges and achieve impact by shaping the future of cyber education and workforce development across AUKUS nations. Specific goals included strengthening efforts to address cyber talent shortages through innovative programs, promoting diversity and inclusion in cyber careers, and building robust public-private partnerships to enhance workforce readiness. Participants also aimed to expand their networks, gain insights from complementary approaches, and influence global strategies for a resilient, inclusive, and future-ready cyber workforce.

CANBERRA MEETINGS AND KEY PARTICIPANTS

The visit included key meetings at several locations in Canberra: the ACT Government International Office, the ASD-ANU Co-Lab, UNSW Canberra/CIT City campus, and UNSW Launch Northbourne Avenue.

Participant representation spanned various sectors:

- **Government:** ACT Government Office of International Engagement, Canberra Cyber Hub, Canberra Innovation Network, Australian Signals Directorate (ASD).
- **Industry and Professional Bodies:** Business Council of Australia (BCA), Future Skills Organisation (FSO), Independent Tertiary Council of Australia (ITECA), Australian Information Security Association (AISA), and the Critical Infrastructure Information Sharing & Analysis Centre (CI-ISAC). Google, Fifth Domain, and MDR Security also participated.
- **Education:** ANU, UNSW Canberra, University of Canberra, CIT, CSU, Western Sydney University, TAFECyber, and Blended Learning International (BLI).

The in-person UK delegation included Mr Chris E (UK NCSC) and Professor Iain Phillips (Loughborough University). Available online from the UK were Ms Steph Aldridge (NeuroCyber, CSE Connect), Dr Charles Clarke (University of Roehampton, CSE Connect), Mr Nigel Jones (Independent Adviser, CSE Connect), and Mr John Madelin (Advisory boards, CSE Connect).

The in-person US delegation included Professor Michael Burt (Adjunct Faculty, NCyTE). Available online from the US were Professor Tony Coulson (California State University, San Bernardino, NCyTE), Dr Deanne Cranford-Wesley (North Carolina Central University), Ms Zoe Fowler (Educational Researcher, NSA-funded Careers Preparation National Center), Ms Amy Maxwell-Hysell (California State University, San Bernardino, CAE Community), Professor Kyle Jones (Sinclair College, NSF/NSA grants), Professor Michael T. Qaissaunee (Brookdale Community College, NSF/DoE grants), Dr. Md Sajidul Islam Sajid (Towson University, CAE-CyberAI initiative), and Dr Costis Toregas (The George Washington University, NCyTE).

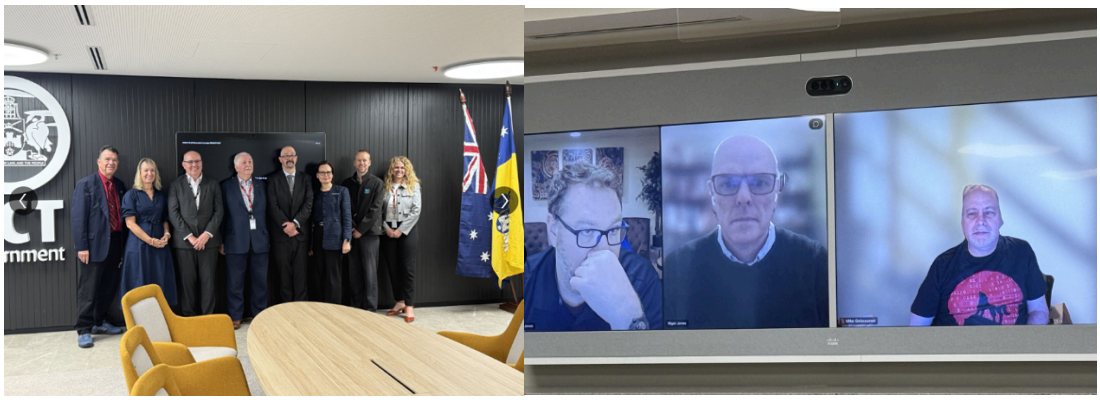
The Australian delegation hosts comprised Professor Glenn Withers (ANU, Social Cyber Institute), Mr Adam Henry (Social Cyber Institute), Professor Greg Austin (University of Technology Sydney, Social Cyber Group) in person, and Mr Jack Goldsmith (Social Cyber Institute, ANU) and Ms Lisa Materano (Social Cyber Institute, Blended Learning International) available online.

Annex A provides short bios of each country delegation and Annex B presents a timeline of discussion and meeting participants throughout the visit's activities.

MEETING HIGHLIGHTS AND THEMATIC DISCUSSIONS

MONDAY, MARCH 17 - ACT AND ANU FOCUS

On Monday morning, March 17, the delegation attended a Welcome and Cyber Sector Landscape Brief at the ACT Office of International Engagement. This meeting featured presentations from Commissioner Brendan Smyth, Skills Canberra, Canberra Institute of Technology (CIT), and the Canberra Cyber Hub and the Canberra Innovation Hub. Dr Vicki Gardner was the lead for the Cyber Hub and Professor Georgia von Guttner for the CIT.

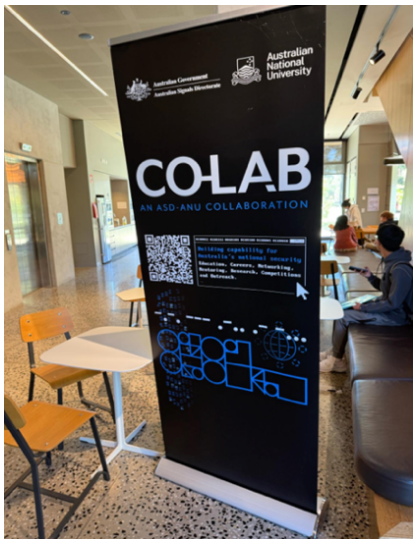


Key strategic level dynamics discussed and noted included **Canberra's thriving information and skills economy** and the **impressive headline relationships among business, government, and academia**. Many initiatives in the region are focused on **relevant education for employment**. This was seen as indicative of moving beyond national and state/territory strategies towards implementation, championed by state/territory government and agencies acting as a neutral 'Switzerland' among diverse stakeholders. This resonated with the **cyber ecosystem approach** to employment, skills, and education development.

Strong **diversity initiatives** with a focus on pathways into cyber and employment were highlighted. There is a focus on **hands-on initiatives** for relevant employment and skills, including bringing industry into the classroom and apprenticeships. Examples given were a Lego model of Canberra for students to practice 'break and defend' scenarios and the 'Academy of Interactive Entertainment' noted for its interest in games, supporting cyber initiatives. These concepts were recognised as engaging, fun, and fostering a competitive security mindset.

Points raised for further discussion stemming from this meeting included **building sub-national and local ecosystems**, how this scales nationally, and how countries internally support or compete with these models. **Apprenticeships, pipelines, and early-stage career opportunities** were noted as structural issues regarding recruitment practice.

However, there is an opportunity to learn from experiences in the UK (and the NCSC in particular), regarding degree apprenticeships and improving the pipeline via the CyberFirst programme. The nature of **core and specialist skills** (business and technical) within the ecosystem and how they should feature in practice was a topic for further thought. Other ideas included **creativity and innovation**, the **economics of arts and culture** informing Canberra's approach (see reporting from Macquarie University), and the concept of **'Skills Activation'** – identifying and developing inherent potential. **Career transition bootcamps** were mentioned, linking to the concept of 'on ramps and off ramps' into and beyond cyber security. **Recognition of prior learning** seemed an important issue for Australians that the visitors felt might be underplayed elsewhere. Lessons could be learned from the Canberra experience with **internships and micro-credentials**. The scope of **wider digital pathways versus specialist cyber pathways** was raised for discussion. The role of **SFIA** (Skills Framework for the Information Age) in Australia was noted as a question for a future meeting.



The afternoon of Monday, March 17, included meetings at the ASD-ANU Co-Lab and the ANU Cybernetics School. At the Co-Lab meeting, discussions touched on the vetting and continuing professional development of cyber security academic staff. From a US perspective it seemed that Australia has a more robust approach to vetting their staff and making sure they do annual professional development. Although the US CAE programme academic staff are vetted there is no mandate that they do annual professional development. The UK perspective was that its approach was more like the Australians.

Co-Lab's focus areas were described as Recruitment, Outreach, Source Training, and Research. The visit highlighted a **unique and distinctive relationship between government and university**, and an excellent example of the benefits that can be realised is the Gemini development programme for analysts. This is open to students undertaking the relevant ASD Honours degree and provides them with the opportunity to undertake relevant research in a secure environment, with a mentor from ASD that has an appropriate background, and a scholarship of approx. AUS$10,000. Jennifer Lawrence led the Co-Lab discussion plus Aruvin Karunakaran.

The meeting at the ANU Cybernetics School included discussions on **AI** and helping people to understand the potential uses and benefits that can be derived from it. Threatcasting was mentioned as a method used to predict future threats with Bryan David Johnson and Jack Blight noted as leaders in this field). Of particular note was how the school deliberately aims for cohorts of students that are as diverse as possible, with

support for ‘non-traditional’ applicants. This leads to a wide mixture of technical expertise and life experiences, with the aim of achieving ‘productive disagreement’ amongst the cohort. Professor Andrew Meares led the Cybernetics group discussions.

TUESDAY, MARCH 18 – GOVERNMENT, INDUSTRY AND FURTHER EDUCATION FOCUS

Tuesday morning included meetings with Australian Government representatives at the UNSW Canberra City campus. This session involved both in-person and on-line participants from Australia and overseas. Introductions were made by representatives from various organisations, including ICEC, Australian Information Security Association (AISA), Independent Tertiary Education Council of Australia (ITECA), Canberra Innovation Network, Loughborough University, Future Skills Organisation (FSO), Fifth Domain, Google Asia Pacific, Business Council of Australia (BCA), National Australia Bank, and the Federal Government's Executive Cyber Council. Innovation Central Canberra was introduced by Frank den Hartog who holds the Cisco Research Chair in Critical Infrastructure at University of Canberra. Innovation Central Canberra caters to non-traditional students through a partnership involving Cisco and 10 universities, offering free access to Cisco courses and research opportunities.

The meeting was a discursive exchange driven by questions, including whether there is a consistent platform for Industry/Education/Government dialogue and engagement in Australia. Insights shared noted that the **Federal, State and Territory system in Australia** results in each state/territory pursuing its own initiatives, presenting a somewhat **fragmented picture** but also allowing diversity and customisation. Similar state dynamics were noted regarding education in the US, but with attempts there at coordination such as through CAEs and NCyTE. The use of **Information Sharing and Analysis Centres (ISACs)** in support of coordination was mentioned. It was suggested that ISACs might move forward in Australia including with the 2024 establishment of CI-ISAC. It was stated that the support for Internships by a former Prime Minister indicated the need and value of having a **champion** for such initiatives. The work of the Executive Cyber Council (ECC), was highlighted in putting together a **playbook of activities/guidance** that has also proven to be successful.

Another key area of interest was the **intersection of policy, practice, and employment**. Specifically, there was curiosity about how language had developed between these communities. The concept of **work roles**, mentioned by a colleague from Fifth Domain, led to discussion about whether this framework was established across stakeholder groups and how such roles are defined (in the US, defined through knowledge, skills, and tasks). A view from an Australian perspective was that the use of **job roles can be problematic in industry**. It would be difficult to find two different organisations in

Australia that would agree on the same cyber security work roles. It was considered **more helpful to focus on tasks** and how those tasks relate to areas like security operations. This task-based approach encourages education to focus on students' ability to complete specific tasks, resonating with the concept of competency being developed and investigated by both NCyTE and CSE Connect[1].

The discussion also turned to the concept of a **cyber security profession** and its development. It was noted that professionalisation is a **complex issue**. The sheer **diversity within cyber security** makes it difficult to view it as a singular thing. If considered a profession, it might be seen as a narrow one involving security operations or digital forensics, with **knock-on consequences for cyber across other disciplines** in engineering, law, retail etc. It was noted that the UK Cyber Security Council is undertaking extensive work in developing the profession and professionalism within the UK, with both NCSC and CSE Connect being closely engaged.

Discussion on **apprenticeship models** noted that US models, such as "truck driver apprenticeship sprints" (used as an example), do not work the same way for cyber security in the US. This prompted a question about what models *could* work. Problems faced by **SMEs (Small and Medium-sized Enterprises)** were raised, with the use of Instagram mentioned as a method to communicate cyber information to them. Lessons might be taken from the **Estonia strategy**, which is able to take a whole nation approach to implement changes effectively. The existence of a **Women in Cyber group** tackling gender imbalance indicated common efforts between the countries towards diversity within the profession.

The framing of the profession, roles, and tasks was seen as a **categorisation and level of analysis problem**. Seemingly diverse fields like AI, Quantum, and Cyber security are all different but are also closely connected when viewed from the perspective of reducing online and cyber harms. This framing presents a significant challenge in public policy and strategy development. There was also discussion on framing cyber tasks in a **competitive context**, seeing it as a contest rather than merely an administrative risk assessment. This relates to developing a **security mindset**, encouraging individuals to understand how to 'break' as well as 'make' systems.

The role of the educator was discussed. While frameworks provide bullet point lists of requirements, the educator's skill lies in developing learning that is based on sound frameworks but is also being **contextually relevant and inspiring for students** while

[1] Subsequent to the Delegation visit, a new integrated cyber warfare workforce strategy has been announced by the Australian Government to enhance multiple career pathway opportunities across all defence service areas: https://www.defence.gov.au/news-events/releases/2025-05-27/investing-australian-defence-forces-cyber-warfare-workforce

meeting employer needs. This requires **support to faculty** (a function that NCyTE provides) and guidance on competency (Zoe Fowler and Vincent Nestlers' ABCDE framework was given as an example). This approach facilitates the translation of requirements into effective course design and necessitates a **partnership between institutions, industry, governments, and students**.

Widely adopted US frameworks were mentioned, including the **NICE Framework Resource Center**, which establishes a common language for cybersecurity work, knowledge, and skills, used across public and private sectors, and the **DoD Cyber Workforce Framework**.

Suggested points to consider from the Tuesday discussions highlighted key tensions and areas for future focus:

- Understanding the cyber education **ecosystem**, which involves forces demanding greater coordination and standardisation alongside forces inspiring regional innovation and autonomy. Are these opposing or complementary?
- How institutions can improve **local industry engagement** and services.
- The ongoing work needed to refine the understanding of **Tasks versus roles versus professions versus other disciplines**, which would benefit from further international dialogue.
- Whether **skills frameworks are often too government-focused** and how to better account for diverse industry needs.
- Methods for developing and instilling the **security mindset and cyber tradecraft**, including the concept to 'Train for uncertainty, educate for uncertainty'.
- The potential **role of gaming** in skills development and activation.
- The importance of **Faculty development** to support contextually relevant education for employability.

Tuesday afternoon involved further meetings with education representatives, including UNSW, Charles Sturt University, University of Canberra, Western Sydney University, and Blended Learning International.

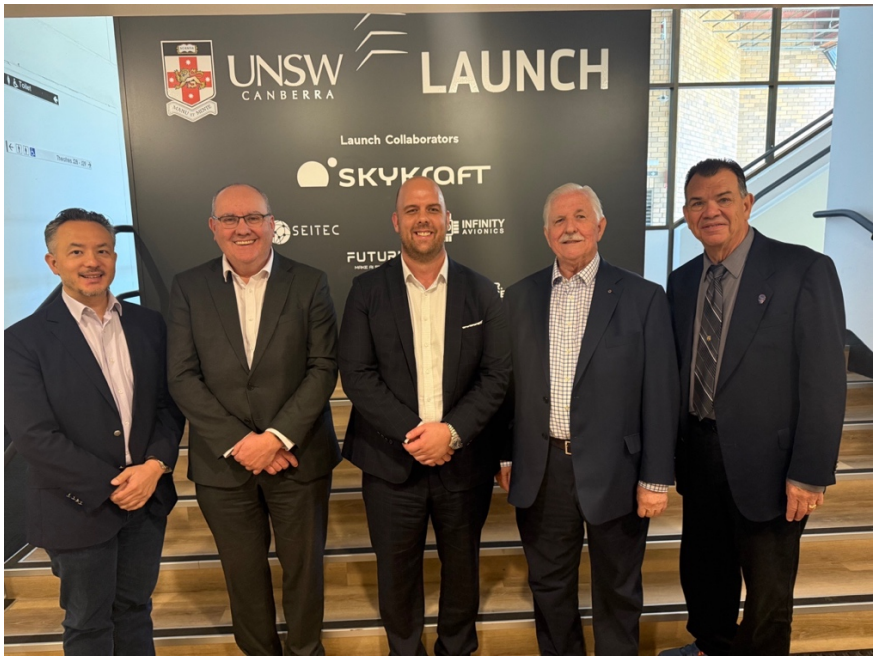
UNSW were represented by Deborah Blackman (Associate Dean for Lifelong Learning) and Ben Turnbull (Associate Professor in Cyber Security). Deborah explained the university's new 'Progress for All' strategy, which seeks to build capability and capacity for industry by helping people to 'come back to' or transfer into the cyber sector. A key component of this strategy is stackable short courses, which allow people from a variety of backgrounds to reach the same level, and/or to target particular parts of the sector.

Ben discussed how UNSW is ensuring that their programmes are mapped to the CyBOK, in a similar way to courses put forward for NCSC certification in the UK, which in turn

allows potential students to evaluate the programmes against their own preferences and ambitions. Chris E2 will follow this up with Ben and the team and introduce them to the CyBOK team in the UK.

With the advent of more advanced and widespread online teaching methods, the group explored the potential of co-teaching. This might see teaching staff from UK/US universities teaching remotely on Australian programmes or vice versa, helping to plug some of the gaps that might exist wrt staff expertise and knowledge, allowing staff to develop and offering students a variety of experiences.

Building on this, an ultimate ambition was seen to be an ongoing joint cyber security education conference, which might run virtually and/or in person, bringing together best practice and practitioners from each nation.



WEDNESDAY, MARCH 19 - COLLABORATION AND FUTURE STEPS

Wednesday morning focused on collaboration moving forward, innovation, industry, and diversity, with international representatives in person and online.

The meeting opened with a presentation from **Matt Wilcox, Founder and CEO of Fifth Domain**, focusing on their **task-based approach to skills development**. His company's approach supports recruit assessment and ongoing management of skills development within a team. It collects data to move beyond subjective assessment of capability to one based on performance captured continuously. This approach is particularly focused on skills associated with **security operations** and building profiles of individuals and teams. More details were available via their website (https://www.fifthdomain.pro).

Matt Wilcox's presentation stimulated significant discussion. A key challenge noted was that **industry certificates** often assess knowledge (frequently via multiple choice tests) rather than actual skills or experience. This reinforced the need, as Matt stated, to assess what people can *really* do, not just what they claim.

Beyond technical capability, a common recruitment requirement is for **soft and cognitive skills**. There is a need to assess the 'whole human', including traits like tenacity and grit. Matt added that **adaptability** is also crucial, citing the ability to pivot on the technology stack during an attack. While soft skills are important, strong **technical knowledge** is essential for effectiveness, and it is demanding.

The discussion highlighted the problem of organisations **looking for "super humans"** when it is often more realistic and effective to **recruit for skills across a team**. The impact of organisational structure on skills, such as a technical CISO reporting to a CIO versus a cyber security lead reporting to a board, was also mentioned. There is a need to **recruit for growth and growth potential** of individuals. The question was posed: is it mastery or potential for mastery that recruiters should seek?

Support for the **development of individuals** through work experience and in their roles is necessary, requiring mentors and senior staff. A related issue is the tendency to place senior technologists into management roles rather than establishing a dedicated technical pathway. Suggested **pathways for development** included technical, management, program management, and governance. A systems engineering academy was cited as an example of good practice in this regard. A career pathway tool developed with US federal money was also mentioned.

Addressing the needs of **SMEs**, it was noted that skills might not be concentrated in different individuals within smaller companies, leading to technical experts being promoted to management or the context favouring "jack of all trades". Using **Associations of SMEs** was suggested as a way to help fill this gap and reduce overhead. Matt Wilcox noted that the Fifth Domain approach can bring new ideas to an organisation. Anecdotal examples highlighted that talent can be found in non-traditional backgrounds, such as a self-taught individual working in a cafeteria who was highly ranked for a SOC role, or a truck driver who topped an NCSC competition event.

A point of discussion was the perceived **unwillingness of educators to adopt new approaches** to assessment, recruitment, and training, with the observation that the most pushback often comes from educators. Early discussions within ICEC had recognised the challenge of industry and educators working together. The focus in ICEC has been on developing this as a **relationship** rather than trying to ‘fix’ each party separately. The question was raised: how can this relationship be further improved and developed?

The need to connect institutions (like CSE Connect, NCyTE and the US CAE Community have aimed to do) was discussed. The visit revealed good examples of **cohesion in Australia in many areas**, offering potential lessons for others through ICEC, with CIT in Canberra cited as an example. Nevertheless, it was recognised there was still much collaborative work to do. Engaging **influencers and key stakeholders**, including international ones, was seen as important. The **rebirth of the CAE program** in the US was highlighted as vital. Its journey, with collaboration being a key community tool, was now expanding into research and other domains. ICEC presented an opportunity for Australia to support the development of a cybersecurity education community, perhaps with an Australian equivalent of NCyTE or CSE Connect.

Structural issues faced by educators and institutions were acknowledged, such as the difficulty in changing approaches to quality, standards, and external inspection; a degree must be assured as a degree. These are **structural problems** requiring systemic solutions, not just changing individual attitudes. Another structural issue identified was the **lack of early-stage career entry points**, which acts as a blocker in the pipeline. Examples like Cyber 9/12 and the UK Cyber Leaders Challenge were noted as initiatives leading on soft skills, policy, strategy, and international issues.

The joint part of the visit concluded with a visit to the Cyber Career Symposium, organised by the Canberra Cyber Hub. This event brought together industry, universities, students and training organisations, plus ASD, promoting career opportunities and options for further learning and training. A mixture of interactive skills sessions, hands-on demonstrations, talks from experts and exhibitor stands allowed visitors to see the local (and wider) cyber security ecosystem in one place, and engage with the various participants.

CONCLUSION AND RECOMMENDATIONS

The Australia ICEC Cyber Education Initiative visit in March 2025 was considered a great success. The early-stage output from the visit looks very promising, indicating a high likelihood of longer-term collaboration between the UK, US, and Australia on cyber security education. The discussions highlighted both areas where Australia demonstrates notable strengths, such as the cohesion seen in Canberra and the ecosystem approach to education and employment, and shared challenges, such as the fragmentation inherent in federal systems and the complexities of workforce development and professionalisation.

The visit provided valuable insights into diverse approaches, including a focus on tasks over roles in industry, innovative hands-on learning, required qualifications for educators, and efforts in skills activation. It also underscored the universal challenges of aligning industry needs with educational output, fostering stronger industry-education

partnerships, and addressing structural barriers in the talent pipeline. The visit successfully facilitated reciprocal fact-finding and laid a strong foundation for future joint efforts.

RECOMMENDATIONS FOR COLLABORATION

Based on the discussions during the visit, the following recommendations for collaboration between the UK, US, and Australia on cyber security education are proposed:

1. **Develop an Australian national community for cyber security education collaboration**: Australia should consider the development of an NCyTE or CSE Connect in order to build on their significant work in developing the cybersecurity education community as well as a way of providing an institutional vehicle to engage with ICEC.
2. **Continue Dialogue on Ecosystem Dynamics:** Further explore the tension between national coordination/standardisation and regional innovation/autonomy in cyber education ecosystems. Share strategies on how these seemingly opposing forces can work together.
3. **Enhance Industry-Education Engagement:** Collaborate on developing models and best practices for institutions (and individual faculty) to improve local industry engagement and the services they provide.
4. **Refine Workforce Language and Frameworks:** Continue the dialogue on the concepts of tasks, roles, professions, and how they relate to other disciplines in cyber security. Work towards a shared understanding or translation framework that better incorporates diverse industry needs alongside government requirements in skills frameworks.
5. **Develop Security Mindset and Tradecraft Training:** Share and jointly develop methods and resources for instilling a security mindset and cyber tradecraft in students, focusing on training and educating for uncertainty. Explore the potential of gaming and skills activation techniques.
6. **Support Faculty Development:** Collaborate on initiatives and share best practices for faculty development programs that ensure educators can deliver contextually relevant education for employability.
7. **Establish Integrated Communities:** Collaborate on creating and developing integrated communities, potentially mirroring or linking existing models like the CAE/ACE community, that actively involve industry partners alongside educational institutions.
8. **Address Structural Barriers:** Share insights and develop joint approaches to address structural changes needed in the education and workforce management

landscape, such as creating more early-stage career routes and exploring flexibility in educator oversight and quality assurance processes.

9. **Explore Data-Driven Approaches:** Investigate and share methodologies for using data-driven approaches and pathway tools to inform better decision-making in recruitment, skills development, and career progression.
10. **Leverage Collaboration Avenues:** Utilise existing structures like ICEC for ongoing information exchange, bilateral discussions, and joint working initiatives. Participate in relevant international events identified, such as the NCyTE CyAD conference, CSE Connect events, HICSS, and Science and Technology Education conferences, to maintain momentum.

ADDENDUM – POST VISIT AUSTRALIAN ACTIVITY

Some initiatives have been taken as follow-up activities looking to future institutionalisation of Australian alliance, commencing initially out of the Canberra cyber community that met with the Delegation,

In particular, the suggestion has been made to link with CSE Connect in the UK and with the National Cybersecurity Education and Training Center (NCyTE) in the USA.

To facilitate, Adam Henry and Glenn Withers have been invited to upcoming CSE Connect and NCyTE linked conference meetings in the US and UK to discuss such alliance further. This depends on finding Australian funding, though other Australian participants from the Canberra meetings are accordingly being invited as well if they have suitable funding in place.

It was noted in Australia that CSE Connect in the UK is funded by their National Cyber Security Centre (NCSC) and that Chris E, Head of NCSC Academic Engagement, who was in the UK delegation to Australia, visited Australian Signals Directorate separately to discuss the visit and their NCSC education programs before leaving Australia.

Accordingly, Glenn Withers has approached Australian Signals Directorate to see if Conference involvement or even attendance could be of interest to ASD, at Moraine Valley Community College in Chicago on June 24-25, and/or the UK event on July 21-23 at University of Warwick. This could be from Australia or by in-country Australian representatives.

Also, the suggestion has been made by Glenn Withers to ASD that, in the longer haul perhaps ASD could consider NCSC-like support for an Australian equivalent to CSE Connect. The March delegation evinced much interest from the entities on both sides for such a development, and the British and the Americans are keen to now take this discussion further as seen in the UK and US meeting invitations.

A further step is to see if some of the other local Australian Canberra parties might be interested in engagement in such a body e.g. CIT, Canberra Cyber Hub, U Canberra, ANU etc., including once ASD attitude and interest is known.

Ideas for a facilitating organisation for cyber education have indeed been advocated in Australia such as by Adam Hanry, but this potential arising from the Delegation Visit for international collaboration adds a new dimension for proceeding. ASD through Redspice and the Future Skills Organisation could fund projects and, indeed, an underlying new organisation itself, and a body such as the Social Cyber Institute could provide that enabling organisation and administration while partnering with the education participants and liaising with industry.

Participation in the US and UK meetings would allow Australia representatives to:

- Judge desire for Australian application to the US and/or UK and /or joint bodies in cyber education
- Learn of the desirable form and nature of the association for this purpose and how they might be funded and operate in Australia
- Define the ambit and operation and activities sought for an Australian organisation to link to the US and UK groups
- Consider prospective affiliates and funding for such an Association
- Discuss the desirability of wider involvement from further allies in cyber matters such as New Zealand and Canada

It would be beneficial to also discuss focus on initiatives in the cross-country alliance of special interest to all parties such as:

- education organisation and structures for cyber education, including issues such as work-integrated learning and internships, recognition of prior learning, micro-credentials and qualification frameworks, professional recognition, public-private partnership. pathways
- inclusion and diversity and skills required within the alliance and for others especially in developing countries, and for special groups such as first nations and veterans, skills for critical infrastructure protection,
- implications of complementary emerging technologies such as AI, Quantum, IoT, and more, for cyber-use including cyber security.

It is noted that there is interest by the parties not only in education delivery but in research. This includes new original research and analysis that informs what is taught. And there is interest in wider community engagement that can be informed and assisted by the education and training initiatives, expertise and focus. This even extends to ideas such as cyber reserves or militia now being examined in Australia through the Social

Cyber Institute, with a particular focus on special group engagement involving veterans and first nation peoples.

ANNEX A: DELEGATION SHORT BIOS

AUSTRALIA

PROFESSOR GLENN WITHERS Professor Glenn Withers is an Emeritus Professor at ANU and UNSW Canberra, with degrees from Monash and Harvard. He has advised Australian and overseas governments and agencies like OECD and World Bank. He is co-founder of the Social Cyber Group and Director of the Social Cyber Institute, researching critical infrastructure, AI, and cyber security.

MR ADAM HENRY Adam P. Henry is a Senior Fellow Partner in the Social Cyber Institute and a policy/program specialist in cyber security education, skills, and workforce development. He has instigated key pilot programs and briefed ministers on these topics. He has a broad cyberspace career across government, consulting, academia, startups, and industry accelerators.

PROFESSOR GREG AUSTIN Professor Greg Austin has diverse international experience in cyber policy research and international security, and is the Advisory Director for the Social Cyber Group and an adjunct professor at the University of Technology Sydney. He has been a Senior Fellow at IISS and Professor at UNSW Canberra, with ten books on international security. He has consulted for UK and Australian government departments and international organizations.

MR JACK GOLDSMITH Jack Goldsmith is an Associate Fellow with the Social Cyber Institute and a Visiting Fellow at ANU's RegNet. His research lies at the intersection of IT, society, and strategy, including cyber security, technology policy, and international security. He writes for Circus Bazaar Magazine and publications like ASPI and the Lowy Institute and recently was awarded the 2025 Munich Security Conference Essay First Prize.

MS LISA MATERANO Lisa Materano is the Director for Education in the Social Cyber Institute and co-founder/Director of the Social Cyber Group and Blended Learning International. She has extensive experience sourcing and providing Executive and Practitioner Programs in Cyber Security globally. Her career spans public sector economics, lecturing, business innovation, and managing large education and training projects.

UNITED KINGDOM

MR CHRIS E Chris leads the Academic Engagement Team at the UK National Cyber Security Centre (NCSC). He builds and develops the UK's cyber security higher education community, fostering collaboration and promoting knowledge sharing. He introduced

and sponsored CSE Connect and has expanded the NCSC certified degree and ACE-CSE programmes.

PROFESSOR IAIN PHILLIPS Dr Iain Phillips is Director of Academic Staffing and Acting Head of Computer Science in the School of Science at Loughborough University, with over 25 years in computer networks research. He has held head of department roles and worked in various engineering and computer science positions. He holds a BSc and PhD from Manchester University.

MS STEPH ALDRIDGE Steph Aldridge is a Director at NeuroCyber and involved in Neurodiversity: Autism into Cyber initiatives. She previously worked at Cyber Security Challenge UK and as Curriculum Manager at Bletchley Park, building the Cyber EPQ. She is passionate about neurodiversity in cyber and co-chairs CSE Connect's Inclusion special interest group with her US counterpart.

DR CHARLES CLARKE Dr Charles Clarke is an Associate Professor and Deputy Head of Computing at the University of Roehampton and co-founder of CSE Connect. He is a cyber security education specialist with extensive experience in IT industry roles including senior management and directorships. He advises government on education initiatives and co-chairs CSE Connect's Innovation special interest group.

MR NIGEL JONES Nigel Jones is an independent adviser, researcher, educator, and writer on cyber security, risk, and strategy. He is interested in social and technological factors shaping risk and has worked across private, public, and conflict sectors. He is a visiting fellow at King's College London and co-chairs the International Cybersecurity Education Collaborative.

MR JOHN MADELIN John Madelin is a founding member of PKI technology in Europe, a Board Advisory member for RSA security conferences, and a growth driver. He has built and run large-scale security services, served as a Business Information Security Officer, and advises on boards for cyber security businesses. He is a Co-Director of CSE Connect and co-chairs the Working with Industry special interest group.

UNITED STATES OF AMERICA

PROFESSOR MICHAEL BURT Professor Michael Burt is an Adjunct Faculty at University of Maryland Global Campus and Wilmington University, retired Full Professor from Prince George's Community College. He has over 30 years teaching cyber security and IT, served as Program Coordinator, and worked with the NSF National CyberWatch Center. He holds MBA and MS degrees, a CISSP, and supported NCyTE grants including CAE mentoring.

PROFESSOR TONY COULSON Dr. Tony Coulson is a professor and Executive Director of the Cybersecurity Center at California State University, San Bernardino. He is recognised for innovative approaches in education and leadership, has an entrepreneurial background, and led research on international training strategy. He leads the National Centers of Academic Excellence in Cybersecurity Community and coordinates over 330 NSA CAE designated institutions.

DR DEANNE CRANFORD-WESLEY Dr. Deanne Cranford-Wesley is the Director of the Cybersecurity Laboratory at North Carolina Central University. She has extensive experience in leadership, curriculum development, and student advocacy in IT education, previously serving as Associate Dean and Department Chair at Forsyth Technical Community College. She holds a PhD in Education Leadership Systems and multiple industry certifications.

MS ZOE FOWLER Zoe Fowler is an educational researcher who has worked with national organisations in the UK and US. For four years, she has been the Principal Researcher for the NSA-funded Careers Preparation National Center, focusing on competency and experiential learning in cybersecurity. She facilitates discussions among educators, policymakers, and employers.

MS AMY MAXWELL HYSELL Amy Maxwell-Hysell is a senior manager for the Centers of Academic Excellence in Cybersecurity Community national center at CSUSB, coordinating with the NSA N-CAE program and over 420 institutions. She has helped secure significant funding and runs national programs including the National Cybersecurity Virtual Career Fair and CAE Symposium. She is pivotal in the CAE Community portal and GenCyber efforts.

PROFESSOR KYLE JONES Prof Kyle Jones is a Principal Investigator and Co-PI on NSF and NSA grants at Sinclair College, serving on NSF National Centers. He worked in IT for over 15 years in various roles and holds multiple CompTIA certifications and an MS in Cyber Defense. He has received several awards and serves on the board of the Go-Cyber Collective and the Ohio Cyber Reserves.

PROFESSOR MICHAEL T. QAISSAUNEE Professor Mike Qaissaunee is Chair of Engineering & Technology and Director of the Cyber Center at Brookdale Community College. He has been awarded multiple NSF and DoE grants focused on cybersecurity education, labs, and K-12 initiatives. He has co-authored an Engineering and Technology textbook and is active in promoting new teaching technologies, receiving several Educator of the Year awards.

DR. MD SAJIDUL ISLAM SAJID Dr. Sajid specialises in System Security, Cyber Deception, and Data Analytics, focusing on Malware Analysis and AI-driven security. His

research leverages AI, machine learning, and LLMs for malware analysis, threat intelligence, and automated defense strategies. He is a Co-PI on an NSF/NSA grant and a lead author for the AI in Cybersecurity framework under the CAE-CyberAI initiative.

DR COSTIS TOREGAS Dr. Costis Toregas is the director of the Cyber Security and Privacy Research Institute at The George Washington University, focusing on education, research, and service projects. His interests include cyber risk assessment, insurance, blockchain, apprenticeships, and utilising Community Colleges in workforce strategies. He consults for NCyTE on international program expansion and advises national governments, serving on several non-profit boards.

ANNEX B - VISIT TIMELINE

Monday, March 17, 2025:

- **10:00 am - 12:00 pm:** Welcome and Cyber Sector Landscape Briefing at the ACT Office of International Engagement (OIE), 220 London Circuit Canberra City.
- Attendees include Hon Brendan Smyth, Emma Gowling, Kiara Papasidero, Dr Vicki Gardiner, Karen Warnes, Professor Georgia von Guttner, Andrew Colquhoun, Kon Vilkov, and a Matt Heffernan (Assistant Commissioner).
- The meeting includes presentations on capabilities and activities from Commissioner Brendan Smyth, Skills Canberra, Canberra Institute of Technology (CIT), TAFE, and the Canberra Cyber Hub.
- A Q&A and discussion session follows the presentations.
- Discussions cover topics such as Canberra's information and skills economy, relationships between business, government, and academia, diversity initiatives, hands-on learning approaches (including the Lego model), and the Academy of Interactive Entertainment.
- Key themes discussed for further consideration include building sub-national and local ecosystems, apprenticeships and early career opportunities, core vs. specialist skills, creativity and innovation, skills activation, career transition bootcamps, recognition of prior learning, internships, wider digital vs. specialist cyber pathways, and the role of SFIA.
- The use of renewable energy in Canberra and the collaboration amongst the city's universities and TAFE are noted.
- **2:00 pm - 3:00 pm:** ASD-ANU Meeting at the ASD-ANU Co-Lab, Level 5, Hanna Neuman Building, ANU Campus.
- Attendees include Jennifer Lawrence, Aruvin Karunakaran, Ed Bertram, and Ashley Rogge.
- The meeting includes a discussion of US CAEs, requiring teaching qualifications and annual professional faculty development for cybersecurity professors, and focusing on recruitment, outreach, source training, and research.
- A tour of the Co-Lab takes place.
- **3:30 pm - 5:00 pm:** ANU Cybernetics School meeting at the Birch Building, Third Floor, ANU Campus.
- Attendees include Prof Andrew Meares, Dr Jessamy Perriam, Katherine Daniell and Lewis Tremayne.
- A very interesting discussion on AI takes place.
- Threatcasting is discussed as a method to predict future threats (mentioning Bryan David Johnson and Jack Blight).
- **5:00 pm - 7:00 pm:** Dinner is arranged.

Tuesday, March 18, 2025:

- **9:00 am - 11:00 am:** Open Discussion Meetings at UNSW Canberra City campus, Canberra City Innovation Precinct (Building J, Room 1.26 CIT Reid Campus, 37 Constitution Avenue, Reid). In person and on-line
- In person attendees include Viren Yerandekar (Host), Felix Perie (ITECA), John Karabin (AISA), Matt Wilcox (Fifth Domain), Rajiv Shah (MDR Security), Jo Cave (VU and Future Skills Organisation), Matt Ryan (NAB), Peter Adamek (CBRIN), Mike Bareja (BCA), and Daryl Periera (Google Asia Pacific) plus Glenn Withers, Adam Henry, Chris E2, Iain Phillips and Michale Burt.
- On-line attendees included Zoe Fowler, Nigel Jones, Costis Toregas, John Madelin, Tony Coulson, Charles Clarke, Steph Aldridge, Amy Maxwell Hysell and Michelle Robinson.
- The meeting is chaired as a discursive exchange of ideas driven by questions.
- Discussion revolves around the consistency of industry/education/government dialogue and engagement in Australia, noting fragmentation across states and similar dynamics in the US with attempts at coordination (CAEs, NCyTE).
- Michelle Robinson notes use of Information Sharing and Analysis Centres (ISACs) for coordination, and Glenn believes ISACs will move forward in Australia, highlighting the value of a champion for internships.
- Zoe Fowler expresses interest in the intersection of policy, practice, and employment, specifically regarding the development of language and frameworks for work roles.
- Discussion highlights the difficulty in defining standard work roles across different organisations in Australia and suggests focusing on tasks for education.
- **11:00 am - 12:00 pm:** Meetings continue in person at UNSW Canberra City campus, Canberra City Innovation Precinct.
- **2:00 pm - 3:30 pm:** UNSW Meeting at UNSW Canberra City campus, Canberra City Innovation Precinct.
- UNSW Canberra attendees include Prof. Chika Anyanwu, Assoc. Prof, Benjamin Turnbull, Peter Adamek, Tom Townsend and Professor Deborah Blackman.
- **3:30 pm - 5:00 pm:** Other Australian Education Representatives meeting at UNSW Canberra City campus, Canberra City Innovation Precinct.
- Attendees include Anna Bohdanets (CSU), Professor Frank Den Hartog (UC), Barkat Abu (UC), Lisa Materano (BLI), and Professor Alana Maurushat (WSU).
- Discussion covers topics such as the professionalisation of cybersecurity, the diversity within the field, apprentice models, challenges for SMEs, the Estonia strategy, women in cyber groups, framing the profession/roles/tasks, framing cyber tasks in a competitive context, the role of educators in translating requirements into learning, and vulnerabilities of a cyber security profession.

- US Frameworks like the NICE Framework and DoD Cyber Workforce Framework are mentioned.
- Suggested points to consider include understanding the ecosystem dynamics, improving local industry engagement, the tasks vs. roles vs. professions debate, developing a security mindset and cyber tradecraft, the role of gaming, and faculty development.

Wednesday, March 19, 2025:

- **9:00 am - 11:30 am:** Launch on Northbourne, 216 Northbourne Avenue, Braddon.
- This session focuses on collaboration moving forward, involving international representatives in person and online participants (ICEC, CSE Connect, NCyTE).
- Follow-on discussions include innovation, industry, and diversity.
- Matt Wilcox (Founder and CEO of Fifth Domain) presents a detailed account of Fifth Domain's task-based approach to skills development, recruitment assessment, and ongoing skills development management.
- His approach uses data to assess performance rather than subjective capability.
- Discussion points raised include challenges with industry certificates assessing knowledge over skills, the need to assess what people can do, the importance of soft and cognitive skills (tenacity, grit, adaptability), the need for technical knowledge alongside soft skills, the problem of seeking "super humans," the impact of organisational structure on skills, the need to recruit for growth potential, the importance of mentor development and technical pathways, and different career pathways (technical, management, program management, governance).
- The role of SMEs and utilising associations to help fill skill gaps is discussed.
- Examples of individuals who were self-taught or in non-traditional roles succeeding in cyber are shared (staff cafeteria worker, truck driver).
- Discussion touches on the perceived unwillingness of educators to adopt new assessment and training approaches.
- Nigel highlights the need to focus on the relationship between industry and educators.
- John asks what can knit together institutions (CSE C, NCyTE, CAE) and the potential role of the visit in Australia's progress here.
- Chris E2 emphasises engaging influencers and key stakeholders.
- Tony notes the importance of the CAE rebirth and collaboration in the CAE community.
- Nigel points out structural issues like quality standards for degrees and lack of early-stage career entry points as blockers.
- Cyber 9/12 and UK Cyber Leaders Challenge are mentioned as examples for developing soft skills, policy, and strategy.

- Suggested structural changes to improve the situation include creating more early-stage career routes, establishing integrated CAE/ACE communities, increasing flexibility in educator oversight, and implementing pathway tools and data-driven approaches for skills and performance.
- **11:30 am - 1:00 pm:** 2025 Cyber Careers Symposium at the Canberra Rex Hotel, 150 Northbourne Avenue, Braddon ACT 2612.
- Hosted by Megan Collins Quinlan (Events Co-ordinator, Canberra Cyber Hub).
- Greg Austin is also present.