NCyTE CENTER

National Cybersecurity Training & Education Center

NCyTE team visit to UK: A cybersecurity education information exchange

Costis Toregas and Nigel Jones

February 2024

London, Manchester, Exeter

The travel described in this report was supported by U.S. National Science Foundation (NSF) Award # DUE 2054724. Any opinions, findings, and conclusions or recommendations expressed here are those of the authors and do not necessarily reflect the views of the National Science Foundation.

Introduction

A delegation from NCyTE, comprising practitioners from community colleges and universities across the United States, visited the United Kingdom (UK) during the week starting November 27th, 2023. This was with a view to scoping and catalysing the potential for a sustainable international collaboration between practitioners and institutions on cyber security training and education. After initial contact with a number of interested educators in the UK through teleconferences, the NCyTE team worked closely in partnership with them to help steer the visit programme and activities towards the project's intended outcomes. This took account of an early understanding of the UK aspirations, interests and aims for such a collaboration.

The US delegation and UK coordinator: (LtoR) Tony Coulson, Nigel Jones, Michele Robinson, Deanne Cranford-Wesley, Michael Qassaunee, Stephen Miller, Costis Toregas, Michael Burt, Amy Hysell; a full list of the US and UK participants is included in Appendix A.

This report outlines the aims and intended outcomes for the visit, the approach taken to ensure those outcomes, the programme, the findings and initial recommendations. It should be noted that it is intended to run a series of on-line follow up meetings with UK and US participants in the visit after this report has been published. This is intended to allow time for further reflection on the visit, to garner feedback from the report, and to discuss next tangible steps.

Context

Whilst few would disagree that international dialogue on security matters is desirable, if not essential, in today's interconnected world, there are numerous tangible and concrete reasons for why this should be emphasized in Cybersecurity training and education, at national, regional, institutional and individual levels.

At the national level we recognize the interdependencies in global information infrastructure through the entanglement of technology, supply chains, markets and services. Writ large, it is in all our interests to address risk in interdependencies by having a skilled and educated cybersecurity workforce. This supports the international development of standards and mutual understanding of diverse risk perspectives. (See US Cybersecurity Strategy and Pillar One UK National Cyber Strategy documents)

At regional levels, we recognize that our communities present characteristics that speak to their specific circumstances. An interesting feature of this visit, as will be discussed, was an introduction to regional differences in the UK and the opportunities for exchange on how to take account of those differences in educational delivery affected by for example, geographical distribution, diversity, socio-economic conditions and job opportunities.

Linked to these regional dynamics is the role of institutions in supporting their local communities and the connections regionally, nationally and internationally. This is particularly with regard to innovation and effectiveness of educational delivery when subjected to resource constraints. Key features of this are in learning how institutions serve the needs of diverse groups, businesses and employers in communities.

Finally, at an individual practitioner level, exchange and collaboration is intended to help their development by placing them in a broad and supportive community of practice. This contributes to one of our core purposes – that of faculty development. It is not only professionally rewarding to interact within a community of practice, it provides tangible benefits in terms of personal development and innovation in practice. It enriches and substantiates the development of an individual within their practice and has direct bearing in the classroom.

It is sometimes said that innovation happens on the margins – for example on the edges of networks. Finding and providing the opportunities for our nations, institutions, and individuals to meet gives innovation the best chance of success through our engagement across real and perceived boundaries.

Visit aims and engagement format

From the outset, the US and UK teams agreed that sustainable ongoing engagement was preferable to a brief information exchange. This had a foundational impact on how we saw the interaction proceeding. It was agreed that exchanging factual information through formal presentations was unlikely to drive progress in itself, even if it revealed some useful nuggets of ideas along the way. Rather, it was decided to exchange where possible factual information ahead of the visit (for example, bios, national documents on programs etc.) so that a shared challenge approach could be the focus of discussion, given the limited time available. This would have two effects. The first was to help systematically identify those shared challenge areas where ongoing collaboration would be fruitful and desirable. The second was a result of framing the visit as the start of something enduring, allowing us to discuss what next and how.

Preparing for the trip, two sets of documents were exchanged using shared folders in the cloud for ease of access. From the US side, biographical sketches of each participant were assembled, along with PowerPoint presentations highlighting the institutional connections and aims for each participant. To prepare the US participants for the complex environment of cybersecurity education in the UK, Nigel Jones (who volunteered to play the role of UK tour coordinator) assembled a briefing book covering the geography, history, educational relevance and current cybersecurity status of each visit meeting place.

The aims of the visit were therefore:

- To form institutional and personal relationships with a view to developing ongoing collaboration on shared challenges in cybersecurity training and education.
- To scope the prospects for engagement at three levels of maturity:
    - 1 – simple exchange of ideas through regular dialogue
    - 2 – the development of joint research and other projects
    - 3 – Institutional development to take sustainable dialogue forward, such as a multinational information exchange forum on cyber security training and education.

These three elements were referred to repeatedly throughout the visits. It was recognized that whilst they show a development in maturity of collaborations, they were not necessarily sequential, but could be addressed, at least in part, concurrently.

Visit program overview

The visit was planned to provide an overview of cyber security education in the UK that illustrated the dynamics at play at the national, regional level and institutional levels, and the relationships between them. This entailed events in London, Manchester (in the North West of England) and Exeter (in the South West of England).

Monday, November 27th

Meeting hosted by the Worshipful Company of Information Technologists (WCIT)

Starting in London, the first event was hosted by WCIT. WCIT is a ‘Livery Company’ based in the heart of London’s financial district, known as the ‘City of London’. It is one of 110 Livery companies concerned with providing ‘a means of guaranteeing the workmanship and trustworthiness of both members and the quality of goods produced’ within their trades and sectors. This mandate aligned well with the US evolving system of “apprenticeships” championed at the national level by government and industry cybersecurity leaders. The system of Livery companies stems from medieval times. WCIT is number 100 in order of precedence. Today it has four pillars of activity:

- **Industry** –to promote and shape the IT industry through neutral forums and links with industry bodies.
- **Education** – WCIT supports several schools, most notably Lilian Bayliss Technology School and the Hammersmith Academy which WCIT helped to build and endow in a joint venture with the Mercers’ Company
- **Fellowship** – WCIT has its own Livery Hall which is used for various events throughout the year – including the hosting the visit of NCyTE.
- **Charity** – the WCIT Charity raises funds and makes grants to charities to promote the use of IT and support the disadvantaged.

In attendance were members of WCIT, London Cyber Resilience Centre, Cranfield University, MK:U, Cyber Girls First, Hays Recruitment, Digital Policy Alliance (DPA), CompTIA, ISACA and Birkbeck, University of London.

WCIT session begins

Presentations were made by:

Jon Kidd, WCIT. Jon introduced the event, providing background to WCIT and highlighting several issues facing the provision of skilled employees, primarily to the City of London. This opened a discussion on diversity, skills and recruitment, touching on ways to provide an attractive and coherent view of the cyber security profession for diverse young people and other career stages. For example:

- Using CSI style digital forensic narratives
- Reframing cyber security as 'digital firefighter' or 'digital nurse'.
- Tapping into 'mission delivery' for example, cyber contribution to environmental issues.
- Bringing cyber to business and other schools at university.
- Discovering talent in the gaming community.
- Taking the experience of, for example, young women regarding online trolling and revenge, and developing responses in terms of counter-tactics and investigations.

James Walsh, Hays recruitment. James provided data on the cyber security skills and employment market. He raised the issue of attitudes of employers towards potential recruits, for example regarding demands for experience and skills in entry-level positions and the 'work readiness' of recruits. Discussion touched on resource constraints in a difficult economic climate, set against the rising risks in, for example, Operational Technology, supply chain security and 3rd party risk. He highlighted the work done by Hays in identifying talent, bringing them into employment and then developing them through the Hays Skills Business. This switched a pipeline model that normally assumes training before employment, to employment before training. In this model, employers have to become **talent creators**.

Pat Ryan, Cyber Girls First. Pat Ryan provided an overview of her Cyber Girls First initiative, comprising volunteer staff supported by corporate sponsors, working to encourage girls to consider a career in cyber security. A dynamic discussion ensued where delegates exchanged information on initiatives that included:

- Code breaking games
- Robotics camps – taking what had been built home.
- Working with youth organisations such as Girl Scouts of America
- Support of national agencies
- Gen Cyber camps supported by the National Security Agency in the US explicitly supporting underprivileged youth in summer camp environments
- The essential task of teaching the teacher and training the trainer, and how that is done and could be done.
- Different funding approaches and economies of scale.

Prof Lynette Ryals and Dr Nikki Williams, Cranfield University/ MK:U. Lynette and Nikki's presentation detailed their degree apprenticeship scheme accredited/ delivered by these institutions. Employees attend a highly innovative programme of education and training. As students are employees, their education is part of their paid work (earning while learning). They accrue no debt in the way that a traditional university pathway would, and it therefore represents an attractive start to careers. Their programme comprises a mix of technical and professional skills, the latter focusing on personal and business skills. A close collaboration between university and business is required. UK funding of the apprenticeship model was discussed, where companies which have annual pay bills (payrolls) over £3 million pay an additional 0.5% of gross revenue as an apprenticeship levy into a digital account. This can then support qualifying apprenticeships schemes undertaken by companies. Unused funds in the digital account default to the Government 24 months after their submission – a kind of 'use it or lose it' motivator.

Zeshan Sattar, CompTIA. Zeshan provided an overview of CompTIA's work in the skills arena, mapped against standards, job roles and career development. A key feature is how beneficiaries of the programme are encouraged to become 'cyber ambassadors' who pass on their expertise and knowledge as part of their commitment to their profession. NCyTE has a set of close relationships with CompTIA in the US and it was useful to make the UK connection.

Mike Hughes, ISACA. ISACA also has its heritage in the United States. Mike discussed a number of features of their work:

- The challenge of core skills for changing needs
- Instilling 'learning everyday'
- Learning from someone else's experience.
- Getting people interested in cyber.

In order to address a number of these bullet points, ISACA has considered a scheme regarding free membership of ISACA for young people.

Meeting hosted by the Digital Policy Alliance (DPA), House of Lords, Palace of Westminster
The meeting was chaired by Baroness Neville-Jones, who is co-chair of the DPA's Cyber Security and e-Crime Group. The DPA 'alerts Parliamentarians and policy makers to the potential impacts, implications, and unintended consequences of digital policies on governance, individuals, society, and business...' it is an '..independent, politically neutral, cross-party broad-based policy membership organisation providing a forum for the technology and digital sectors…' it is…'not a lobbying group'.

This evening meeting was attended by political, academic, public and private sector representatives and industry bodies. A range of practical challenges were discussed, including shared challenges and approaches taken in each country. Of particular note were three discussions

> One on recruitment, vetting, employment and retention.

> Another on apprenticeships/ internships. This also involved the discussion of industry and student expectations regarding work readiness.
> A third related discussion involved diverse models of cyber security education including micromodules and community based SOCs supported by colleges and industry to help provide trained people into the workforce.

MIchele Robinson and Baroness Neville-Jones

Tuesday, November 28th

Meeting with the UK National Cyber Security Centre (NCSC) and CISSE UK, Manchester

The NCSC is part of the UK's technical intelligence agency, GCHQ. This is the UK equivalent of the National Security Agency. NCSC acts as the National Technical Authority on cyber in the UK. The NCyTE team met with a representative of NCSC's education team. A full and free exchange was had regarding programmes based around respective versions of Centers of Academic Excellence (CAE)/ Academic Centres of Excellence (ACEs), diversity and young peoples' programmes, the cyber body of knowledge and relationships with professional bodies. Charles Clark from CISSE UK discussed their frontline impact approach to supporting educators and students. CISSE UK (potentially rebranding shortly) works closely and is funded by NCSC. Much of their work has used the concept of developing a 'Problem Book' to work as a community on addressing those problems. This includes the Cyber Security Education problem book (https://www.cisseuk.org/the-cse-problem-book). This encompasses a wide variety of themes including, for example:

- Establishing and maintaining collaborative initiatives with industry.
- Improving the accessibility, relevance, and impact of cyber education programmes across all education key stages.
- Providing students and career changes with innovative and authentic learning experiences.
- Increasing the number, scope and variety of internship and job placement opportunities for students and career changers.
- Enhancing the provision of mentoring and careers guidance initiatives for students and career changers.
- Enhancing outreach and advocacy in cyber security education.
- Improving the scope and scale of equality, diversity and inclusion in cyber employability and job roles.
- Enhancing and increasing the scope, scale, and methodologies for evaluating and measuring the impact of trends in cyber education.

Manchester discussions

The US delegation also discussed a range of online resources including EMATE interactives, the CLARK Cybersecurity Curriculum Digital Library, which contains a repository of learning resources, and the NICE Challenge Project, which provides realistic work experience through virtualized environments. NICE has the benefit of providing data about levels of skills and knowledge to students and educators.

A wide range of topics were discussed throughout the engagement including for example:

- Outsourcing to others (academia and non profits) for CAE evaluation
- Two year and four-year degree approaches to education, subsequent to school education.
- Innovation in cyber security education and curricula.
- Virtual career fairs, camps and Gen Cyber for middle school students
- National Crime Agency (UK) and FBI engagement with skills and talent.
- International students and specific challenges around clearances
- Cyber security competitions, such as the National Cyber League
- Relationships with business.

The US delegation had the opportunity to brief on and discuss the potential for ongoing collaboration along the lines of the three levels of maturity mentioned above.

Wednesday, November 29th to Friday, December 1st

During this period three roundtable meetings were held in Manchester, Exeter and London, each of which were co-chaired by a UK and US participant. The roundtables had a regional focus in order to identify and take account of the different characteristics of local communities, and how this might be reflected in the provision of cybersecurity educational activities, now and in the future. Each roundtable was given a working, albeit interrelated theme, in order to vary the discussion and focus between roundtables, but also grounding discussion on dynamics considered to be locally important. Consequently:

> **The Manchester Roundtable** theme was ‘Creating a diverse and connected cyber security community’, given the UK national initiative to locate both a new office for GCHQ/ NCSC in Manchester, and the National Cyber Force, further north, thereby creating a regional need for skills to fill jobs and connect the community along what has become known as the North West Cyber Corridor. This was in the context of addressing a ‘north-south divide’ in the UK, and attempts to bolster the economy of the North West, in the post industrial era.
>
> **The Exeter Roundtable** theme was ‘Providing/ Developing knowledge and skills for business and innovation’. This was driven by two regional characteristics. First was the hosting of the event by the South West Cyber Security Cluster (SWCSC), focused on skills and security for small business and innovation in cyber technologies. The second was the presence of Bristol University in the region which is the lead institution for the UK’s

Cyber Body of Knowledge (CyBOK). The South West has diverse characteristics in terms of sectors served in towns and cities separated by largely rural and agricultural communities. Population dynamics tended to show an older population (10 years on average compared to London) with pressure for opportunities for young people in a tourist rich, second home owning region.

The London Roundtable theme was ‘University outreach in cyber security and skills for local communities in a global city’. This was to examine how universities could work with local communities to service their needs and the needs of a large financial sector. This dovetailed with much of the discussion in London earlier in the week, but attempted to make diversity and inclusion a specific focus of the discussion of local dynamics in the boroughs of London which exhibit extremes of poverty and wealth, alongside uneven density of ethnic diversity, in the most ethnically diverse city in the UK (or even the world).

The Manchester/ North West Roundtable

The Manchester event had representatives from five universities in the region, plus NCSC, business and public sector representatives. The venue was Manchester’s new Digital Security Hub, a partnership of government, business and universities.

time is what determines security. With enough time nothing is unha ble.
Welcome to Greater Manchester Digital Security

Manchester Roundtable

The following challenges were raised by individuals around the mixed US/UK tables:

- Funding models for educational initiatives
- More women in cyber, more diversity (see me, be me)
- SME scalability issue regarding cyber responsibilities, knowledge and expertise
- What works, what do we know works? (The rising tide lifts all boats…)
- How do we measure success – e.g. at a student level, where are they now? ROI?
- The need for innovation in cyber education
- Use of extended reality and other technology
- The pipeline/ conveyor belt/ highway ramps challenge - from talent identification to work and beyond.
- The NW pipeline/ corridor – protect the NW, reflect the NW, connect the NW (Protect, Reflect, Connect)
- Recruitment and retention of university staff.
- Social mobility through cyber security – breaking the cycle of low attainment and moving people up.
- Developing good industry projects and retaining good students.

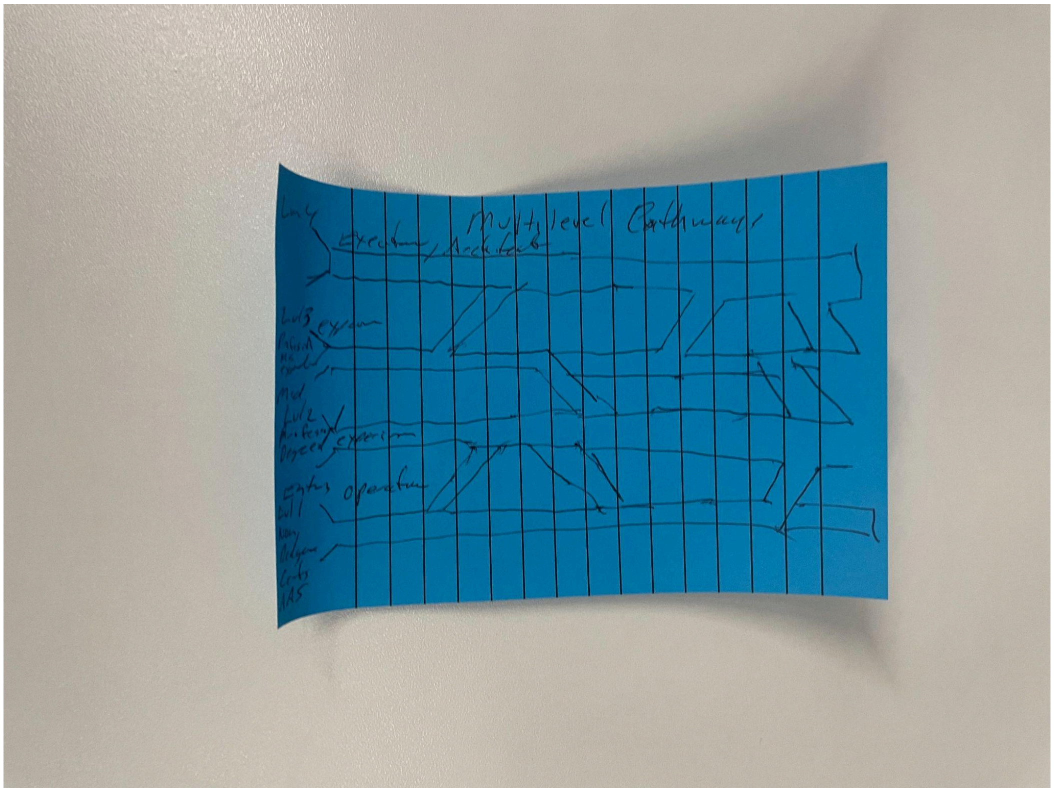
A number of these challenges were down-selected for examination and a further task framed as 'Map the conveyor-belt on the NW community – what does it look like?' This was a deceptively challenging task as it required participants to think about how a seemingly linear process was mapped against a networked community. A fascinating set of insights emerged alongside a set of exchanges regarding current initiatives and innovation. Two major themes emerged:

1. Whilst pipelines and conveyor belts are useful metaphors for work force development that are explanatory and helpful in some ways, more value seemed to be derived from thinking of identification and engagement of talent, as a network of highways with on-ramps and off-ramps – and maybe even diversions.

2. Following on from this, there was an engaging discussion on what those on ramps and off ramps looked like. A key characteristic that emerged was based on the idea of decision points in an individual's or organization's life. Some of these were formal and easily identifiable, such as transition between different phases of schooling. Others were more event driven such as when a company has suffered a cyber attack - 'a visceral moment'. Others included an individual child having a changing life event, such as the loss of a parent or becoming a caregiver. A natural extension of this discussion considered the touch points and timely salience of engagement and communications relating to decision points, educational models and cyber careers. There was clearly a large range of 'ramp' decision-points including:

    a. Veteran's choices
    b. People coming in and out of industry
    c. Companies growing their own talent
    d. Phases of parenthood

e. Innovation hubs and opportunities
f. Where and how people are engaged for age, gender, ethnic and neuro diversity.
g. Seedlings – whilst in study – mentoring, investments, aiding transition
h. Neuro-diversity diagnosis and visualizations of opportunities and circumstances (tools)
i. Conversion pathways for skills



Group synthesis of ramps

A number of fundamental conditions shape such dynamics, including:

- Community engagement is not one visit – it is continuous.
- Giving students agency and a confident voice
- Making sure that interventions do not make matters worse.
- Breaking the myths regarding certifications/ promoting stackable credentials as an alternative?
- Incentivizing faculty extra-curricular activity
- Promoting problem-based learning in connection with fitness for work, and the changing cyber environment.
- Exploiting the power of games.
- Developing ways to maintain the currency of curricula in a fast-moving environment.

- Developing a community of practice for cyber security educators and the challenge of multiple repositories of information and support – in different continents.

A further discussion ensued about the nature of future collaborations to address the above. Once more the three levels of maturity were invoked with potential tasks including:

- Content sharing activities
- Repository mapping - perhaps using AI assistance
- Webinars, seminars, symposia, and summits
- “5 Eyes” cybersecurity education community development
- Mapping journeys to cyber
- Understanding on-ramps and off-ramps – as above.
- Reviewing CyBOK from an international perspective.
- Social mobility focus and mapping opportunities.

The Exeter/ South West Roundtable

Hosted at Exeter University, three regional universities were represented alongside other educators, innovators and industry representatives. The following challenges were highlighted around the table of UK/US delegates:

- The diversity challenge - one that is a societal, organizational and individual challenge - what am I doing about it?
- Understanding the underlying reasons behind diversity gaps. (Progress compared - US to UK?)
- Creating a network foundation that is diverse in terms of culture, gender, neuro, ethnicity, through all career pathways.
- The geographical challenge for widely distributed communities
- Performance measurement of interventions and initiatives
- STEMM Challenge - as championed by ‘Athena Swan’ - https://www.advance-he.ac.uk/equality-charters/athena-swan-charter
- Moving people from talking to doing!
- Institutional challenges in collaboration
- Employers attitudes - see a skills gaps but don’t want to participate, yet expect experience and work-ready starters.
- The need to deliver training differently to safety diverse circumstances: the one-size-doesn’t-fit-all problem.
- Cyber is seen as something for other people - difficult for small businesses and charities. Even in large businesses, it is ‘done by the people over there.’
- Language challenge - we are talking about concrete problems with an abstract technical language.
- Cyber for the masses - not just for classes - social mobility.

- Democratizing learning about cyber security: reaching into communities, selection processes, identifying critical thinking.
- Pedagogical techniques for changing circumstances in cyber, whilst understanding Cyber foundational concepts (that don't change so quickly).
- Job descriptions and HR issues.
- Cyber as a marketing problem - the 'power of why', thinking cyber as resilience of society and business - reframing.
- Thinking of people and cyber security education - before, during and after - the golden thread.
- Retention of faculty staff.
- Students who want a job in cyber security but don't want to go to University.
- The need to look at the cyber eco-system systematically rather than as individual parts.
- ESG - realizing the social value of cyber-security.

Exeter Roundtable

After the interval Professor Rashid, University of Bristol, provided a short presentation on CyBOK. CyBOK can be viewed at https://www.cybok.org/ . He highlighted the free resources available online. In response the US delegation presented a number of online repositories, such as EMATE interactives, CLARK, NICE Challenge and Try Cyber. Following this a number of discussions took place on down-selected challenges.

Innovation in cyber security that takes account of geographical distribution

There was a discussion about the completely online approach taken by Eastern New Mexico-Ruidoso, in support of its 20,000-population occupying nearly 5000 square miles of land, including large expanses of Lincoln National Forest and Mescalero Apache Reservation. As a consequence, the student population has attracted on-line students far beyond the local community, and now includes both other US and international students, as well as home-schooled students. Work has begun on creating a cyber range and a Security Operations Center (SOC) that will support local tribal business interests as well as provide student training facilities.

In the UK, most universities were able to pivot towards online services as a requirement of the COVID pandemic. There is significant use of virtual machine infrastructure which has several advantages for individual and collective learning; laboratories; isolated, non-operational environments; and the creation of configurable diverse infrastructure. This allows any group to learn on any hardware at any time of day. Students can access from home and reserve physical computers onsite. There was discussion of how students were involved in live projects, offering assured service to businesses, at cost-effective rates. Plymouth University discussed their CyberSHIP project as an example of university-business collaboration - and an example of a sectoral approach to cyber security education and research.. (https://www.plymouth.ac.uk/research/cyber-ship-lab)

Diversity

A number of points were debated regarding diversity:

- How to develop more push from parents for their children to enter cybersecurity.
- How to grow aspirations through early engagement
- How to run camps and summer schools, such as Gen Cyber
- How to develop pathways to cyber security through university outreach to business in support of their programs.
- Exploring opportunities to grow with local government support.

Performance and outcome measurement of cybersecurity educational interventions

Two main themes arose during this discussion on how to measure:

1. Economic impact
2. Generation of interest in programmes

Regarding the first, a top line measure was an increase or decrease in unfilled jobs. Regarding the second:

- Would a student recommend the course to someone else?
- A social contact to 'pay it forward - would a student consider a programme a down payment in giving back? This also included the notion of a culture of 'service learning' where experience and theory are combined through project and volunteering efforts, in the local community for charities, businesses and other bodies.[1]
- Industry satisfaction with courses, support and students
- Refined feedback loops to support the next iteration of the course.
- Students' whole learning journey should be tracked to find 'tomorrow's talent', where for example 'a young person shows talent, but can't do interviews.'

The London Roundtable

The London Roundtable was hosted at King's College London (KCL). Participants comprised academics, university strategists; the Chartered Institute of Information Security (CIISEC); diversity champions covering both gender and neurodiversity; The Cyber Security Challenge competition; an FE college offering its online services to others in a consortium, a number of KCL MA students; and other public and private bodies. The opening personal introductions and discussion previewed a wide range of issues including:

- Social mobility - KCL and California State San Bernardino compared - Hyperdiversity and social mobility in London - KCL one of the most socially mobile universities. California State, San Bernardino moving up the social mobility rankings. Importance of career fairs run by San Bernardino. Leading the cyber effort across 23 California State campuses.
- Keen interest in transition between school and university - degree awarding powers in the UK lie mostly with universities
- Role of community colleges in the US, and Whatcom Community College of national importance for CAE candidates and Cybersecurity Education, through federally funded projects.
- Tensions between commercial sectors and national security needs in terms of approaches, attraction incentives and competition for talent.
- Chartering (through Chartered Institutions) as an approach to sectoral standards and behaviors. This led to a discussion on legal liability of chartering bodies.
- Five Eyes discussion - On one hand, a ready made platform for adding a continuous dialogue on cyber security education. On the other hand, the Five Eyes community is the high-end security sector at the top of the pyramid - it's trying to reach below that to the broader base of the pyramid. A discussion followed on recruitment and interest of the few, the many and the all.
- Finding ways to attract good faculty, retain and help them grow professionally.

[1] Afternote: For more information on service learning in relation to cybersecurity, this paper is helpful: Kembley Lingelbach, Student perceptions of a cybersecurity service-learning project, *Issues in Information Systems*, Volume 22, Issue 3, pp. 307-319, 2021

- Funding models for consortium working - problem of getting stuck with Financial Directors in the US (and in the UK?) in distributing (or more to the point, denying) resources.
- What are the community, non-institutional based models for improving collaboration, trust and dialogue?
- Innovation on how we teach cybersecurity required.

King’s Roundtable

Challenge discussion

A further period of discussion raised the following challenges:

.

- Pipeline issues regarding talent identification and development.
- The breadth of cyber security - more than a computer science lens. Integrating technical, managerial and business strategy. What was considered core and specialist knowledge is changing in today's data driven, connected environment. Some of this is hampered by reporting lines for cyber staff regarding senior leadership in organizations.

For young people too, we need to communicate that Cyber is not a specialist function - it underpins everything about how society (and companies) function.

- Challenges associated with diversity, social mobility and the role of competitions. Trust is a key problem that also affects diversity. We trust people who look like us. This feeds into delinquency and gaming, for example, the ethics of breaking and hacking systems.
- Performance measurement of interventions and of students - how to assess student's competency.
- Diversity and gamification, diversity and pipeline, diversity and job opportunities - diversity as an integrated rather than separate topic.

Following the challenge discussion, three topics were identified for more detailed discussion. The table below summarizes the Roundtable output in terms of potential future collaboration, a format that has been developed further in the report, as a way of presenting the potential collaboration opportunities identified through the whole week.

Group discussion output - regarding possible future collaboration

	1	**2**	**3**
Discussion Topic **Maturity level/ bucket**	**Pipeline/highway/diverse/social mobility/engage business/skills base**	**Define cybersecurity broadly for topics and participants and organization development role**	**Teaching innovations: how/what we teach/games/competitions /AI**
Information exchange	On the ground and day-to-day	Study consortia operation	Innovations can apply to classrooms/recruitment/ extra-curriculars. Share existing innovations within countries and cross-countries.
Joint efforts	Across industry, academia, NGOs and government	Find the framework and make them relevant	DARPA project to build virtual spaces for modeling and simulation of games etc., and allow them to be rapidly customised so environments are more familiar and relevant for students.

Institution building	Communication gap: how do I know I'm invited to that party/field? Bring WICIS and WICIS UK together.	Shared resources – a way of building on the efforts of different participants to then share resources round. California example of resource-sharing tool here.	Involve career advisors, parents, students themselves. Ask the right questions of the students if you want to get this right. Get teacher buy-in as they need to shepherd the project.

General observations

From the rich conversations, the following observations are emerging that can guide further steps:

- Clearly shared challenges
- desire to collaborate
- some quick wins
  - Bilateral activities that are being formed organically from the exchange so far (Pat Ryan + Deanne Crawford-Wesley, Peter Trim + Stephen Miller, Clare Johnson activities, Tony COulson from CAE Community and Pat Ryan regarding Gen-Cyber)
  - discussions with government officials regarding ongoing or expansion of activities
- long list of ideas and challenges as a starting point for agenda setting

Recommendations

Recommendations for moving forward will be developed after a UK-US online discussion at the end of January 2024 along the lines of the agreed three dimensions of collaboration

> Continued exchanges and sharing of existing frameworks, curricula and instructional resources and tools.
> Joint activities of mutual benefit, such as collaboration on research projects, articles and paper development, linking specific initiatives across the Atlantic (such as CAE-C linking Pat Ryan with the Gen-Cyber team for mutual gain) and presentation proposal development and delivery at virtual and in-person conferences.
> Explore the establishment of a new alliance structure or integration of academia with an existing alliance structure (such as 5 Eyes for Academics) to keep our progress moving forward.

Appendix A: Participants in the US Visit to the UK

Title	First name	Surname	Organsiation	Delegation
	Steph	Aldridge	Cyber TBC	UK
	Rob	Aspin	University of Central Lancashire	UK
	Matt	Beck	Heart of Worcestershire College/ BLC	UK
	Achim	Brucker	Exeter University	UK
	Michael	Burt	NCyTE	US
	Charles	Clarke	CSE Connect	UK
	Nathan	Clarke	Plymouth University	UK
	Jim	Collins	King's College London	UK
	Simon	Cook	Lancaster University	UK
	Tony	Coulson	California State University, San Bernardino	US
	Deanne	Cranford-Wesley	North Carolina Central University	US
	Daniel	Dresner	Manchester University	UK
	Chris	E2	National Cyber Security Centre	UK
	Amanda	Finch	Chartered Institute of Information Security (CIISEC)	UK
	Steve	Furnell	Nottingham University/ CIISEC	UK
Dr	Bogdan	Gita	Plymouth University	UK
	Mike	Halliday	TechEd Pro	UK
	Mike	Hughes	ISACA	UK
	Amy	Hysell	California State University, San Bernardino	US
	Roy	Isbell	WCIT	UK
	Andrew	Jackson	Salute My Job	UK
Dr.	Clare	Johnson	Women in Cyber	UK
	Nigel	Jones	Right Objective Ltd/ King's College London	UK
	Jon	Kidd	Worshipfull Company of Information Technologists (WCIT)	UK
	Robin	King	Bar Associates/ SWCSC	UK
	Ji	Li	WCIT	UK
DCI	Chris	Maddocks	North West Cyber Resilience Centre	UK
	John	Madelin	Cambridge MC/ Cyber Balance	UK

Title	First name	Surname	Organsiation	Delegation
Dr.	Ashwin	Mathew	King's College London	UK
Professor	Stephen	Miller	Eastern New Mexico University, Ruidiso	US
Supt	Mark	Moore	South West Cyber Resilience Centre (SWCRC)	UK
Dr.	Mustafa	Mustafa	Manchester University	UK
Baroness	Pauline	Neville-Jones	Digital Policy Alliance	UK
Dr.	Bob	Nowill	Cyber Security Challenge	UK
	Tim	Parker	SWCSC	UK
	Annabel	Plews	King's College London	UK
Professor	Michael	Qassaunee	Brookdale Community College	US
Professor	Sara	Rankin	Imperial College London	UK
	Awais	Rashid	Bristol University/ CyBOK	UK
	Geoff	Revill	SWCSC	UK
	Michele	Robinson	NCyTE	US
Professor	Lynette	Ryals	Cranfield University/ MK:U	UK
	Pat	Ryan	Cyber Girls First	UK
	Zeshan	Sattar	Comptia	UK
	Keith	Simson	Kestrel Education Consultancy	UK
Dr.	Tim	Stevens	King's College London	UK
Professor	Andrew	Stewart	Manchester University	UK
	Ashley	Sweetman	King's College London/ Standard Chartered Bank	UK
Dr.	Costis	Toregas	NCyTE	US
Dr.	Peter	Trim	Birkbeck, University of London	UK
	Meropi	Tzanetakis	Manchester University	UK
	Philip	Virgo	London Cyber Resilience Centre	UK
	Arthur	Virgo	Digital Policy Alliance	UK
	James	Walsh	Hays	UK
Dr.	Niki	Williams	Cranfield University/ MK:U	UK
	Tom	Zebedee	OFSTED	UK