NCYTE CENTER
National Cybersecurity Training & Education Center

CSE CONNECT

THE ROLE OF INTERNATIONAL COLLABORATION IN CYBERSECURITY EDUCATION

Building a Global Cyber Workforce:
Innovation and Collaboration in Cybersecurity Education

JANUARY 2025

AUTHORS

Costis Toregas
The George Washington University

Tony Coulson
California State University, San Bernardino

Nigel Jones
CSE Connect (A National Cyber Security Network)

IN THE REPORT

ABOUT THIS REPORT

This report examines the importance of international collaboration in addressing the global cybersecurity workforce gap. It focuses on the formation of the International Cybersecurity Education Collaborative (ICEC), which connects educators, industry, and government to share best practices and tackle challenges in cybersecurity education. By fostering innovation, inclusion, and industry relevance, ICEC aims to develop a skilled, global cyber workforce to meet evolving security needs.

ABSTRACT

Cybersecurity demands constant innovation and adaptation to change. There are no geographical security borders and boundaries with Internet connected/enabling technologies. In the context of teaching and learning, one must consider:

- **Technology enabled education that engages learners (in class and remotely, in groups and as individuals, in knowledge, skills and competency)**
- **Technology innovation that creates realism in cybersecurity practice (cyber ships , power plants etc)**
- **Technology enabled management of learning**
- **Educational and technological responses to the malign innovation of bad actors**
- **Process innovation**
- **Innovation in exposing students to complexity for the purposes of developing higher order thinking skills (beyond predictable patterns of trained behavior.)**
- **Workforce needs of business and industry, including those that operate globally or draw on an international supply chain.**

DRIVING INNOVATION IN CYBERSECURITY EDUCATION

"Cybersecurity education must evolve alongside emerging threats, integrating technology-enabled learning, process innovation, and workforce-driven strategies. International collaboration, like the International Cybersecurity Education Collaborative (ICEC), is essential for shaping the future of cybersecurity talent and research."

As innovation happens on the boundaries of different ecosystems, a possible source is in the creation and support of international networks of academic leaders who face the double task of creating workforce, as well as researching new solutions. This challenging imperative can be helped through international collaboration, and one such effort to create the International Cybersecurity Education Collaborative (ICEC) is described here.

INTRODUCTION

Cybersecurity issues have become an international concern, as evidenced by daily news reports of massive hacking attacks targeting critical infrastructure, healthcare, and financial sectors.

The proliferation of these attacks has further intensified the perception of a cyber workforce crisis, a problem that has been a persistent issue for decades, with industry, academia, and government all acknowledging and attempting to address it. In the United States alone, there are an estimated 457,000 open cybersecurity positions (cyberseek.org, Nov 2024), while globally, the problem is estimated to be at 4.76 million (ISC2 Cybersecurity Workforce Study, 2024).

While agreeing that not enough cyber workforce is being produced given the threat landscape, actually creating a cyber workforce is not a simple task. Many efforts exist from within national governments, industry, and academia, but the growth in the cyber workforce gap increased 19% (ISC2, 2024). The challenge to solve this problem is not just a one-time effort; a mechanism needs to be created for a workforce in a field that is constantly changing while maintaining a pathway to ensure a constant inflow of talent.

In 2023, the Office of the National Cyber Director within the Executive Office of the President (White House) released a National Workforce and Education Strategy where it was suggested that there be a national and international push to foster collaboration between employers, educators and government, including the development of cyber education ecosystems. The creation of a robust, resilient cyber workforce is not a simple task and involves a multitude of entities: educators, learners, employers, government, unions, private training providers, philanthropies, and trade associations. But more importantly, given the international nature of cyberspace, we must seek to learn from like-minded international partners how they have built their ecosystems, learning best-practices, and sharing solutions to help solve a common problem.

Educators in academia, the main “producers” of cyber workforce talent, play an important role in promoting the exchange of ideas, practices, and strategies to bridge the cyber talent gap. As innovation happens on the boundaries of different ecosystems, a possible source is in the creation and support of international networks of academic leaders who face the double task of creating workforce, as well as researching new solutions.

Similarly, efforts in the UK have been shaped by, for example, the five pillars of the UK National Cyber Strategy 2022. The first pillar is 'Strengthening the UK cyber ecosystem, investing in our people and skills and deepening the partnership between government, academia and industry.' This has entailed investment in sustaining Academic Centres of Excellence and certification for degrees; the creation of a chartered body for the cybersecurity profession; and efforts to grow the supply of cyber skills and ensure their relevance and diversity. The fourth pillar focuses on global leadership, and aims to implement measures to improve partnerships and collective actions to reduce up-stream threats.

Both countries have understood that no single entity can help develop the workforce needed for the future. It will take a network, systems approach which is shown in the diagram below:

Clearly the importance of diversity in group thinking, and the multiplicity of ways of attacking problems is important to arriving at innovative solutions and is one of the founding principles of ICEC. This benefit of diverse thinking that comes from international networking includes expansion/ inclusion of partner nation states in the effort and provides guidance for careful expansion.

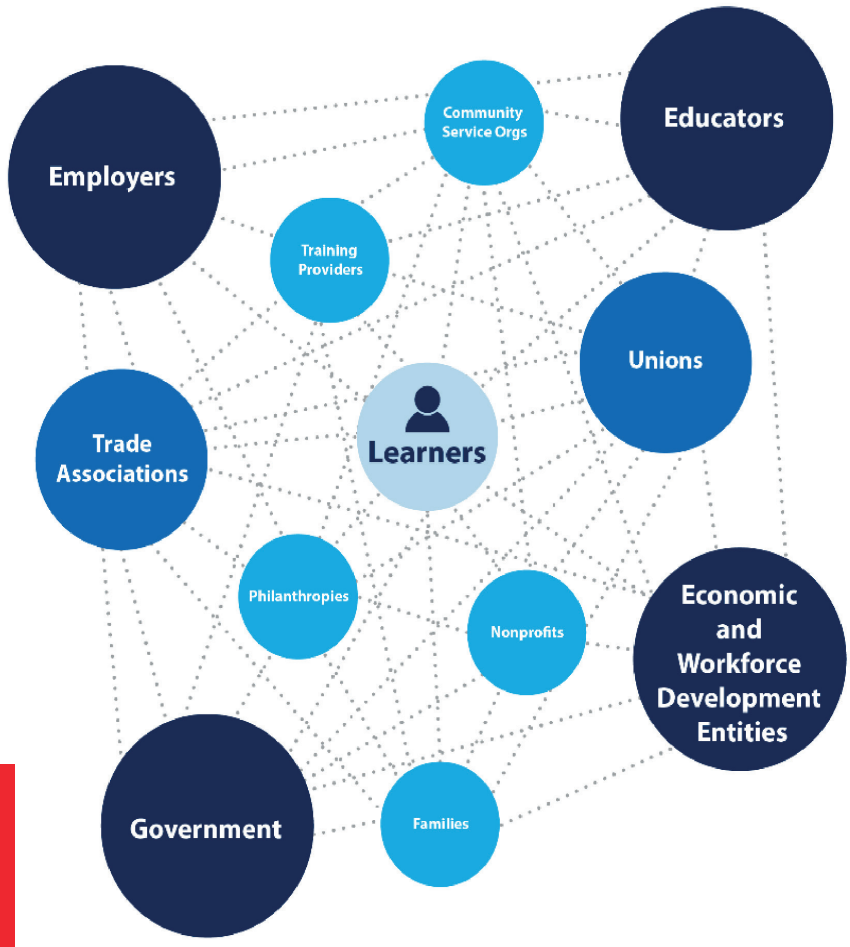

Figure 1. *Example of a Cyber Workforce and Education Ecosystem. Find more examples at https://whitehouse.gov/cyberworkforce*

UK-US CONNECTIONS

ORIGINS OF ICEC

The origins of ICEC stem from a visit to the UK in November 2023, by an NCyTE team representing a number of institutions. 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 education information exchange 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 cybersecurity 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 cybersecurity 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).

DOCUMENTATION AND DISSEMINATION OF TRIP

A report describing the goals and actual achievements of the trip was written by Nigel Jones and Costis Toregas and is archived here (https://www.ncyte.net/home/showpublisheddocument/420/638441147453600000) freely available to the public. NCyTE and CSE Connect are making efforts to circulate the report to interested parties that may be ready to invest time and effort in broadening the ICEC effort.

BUILDING LASTING UK-US CYBERSECURITY COLLABORATION

"Rather than a one-time exchange, the UK-US cybersecurity education visit was designed as the foundation for sustained collaboration. By identifying shared challenges, exchanging key information in advance, and structuring discussions around ongoing engagement, the initiative set the stage for deeper institutional partnerships, joint research, and a multinational cybersecurity education forum."

ICEC FORMATION

A key driver for the formation of ICEC was the desire to sustain a collaboration between the US and UK.

The US and UK were fortunate to have national institutions fostering networks of cybersecurity educators, namely NCyTE and CSE Connect respectively. CSE Connect in the UK quickly agreed to support the initiative having participated in the NCyTE sponsored US visit to the UK. The two organisations developed an informal dialogue and agreed the collaboration would be beneficial, and that resources and costs would in principle lie with network members of NCyTE and CSE Connect, if and when they wished to participate in international activities. A light touch secretariat was formed between the two organisations, and co-chaired by UK and US representatives, comprising considerable volunteer effort and small budgets dedicated to international outreach.

Nevertheless, beyond critical institutional support, some structured thinking needed to be applied to how collaboration would happen regarding the shared areas for interest. In part the leadership turned for inspiration and insight from current thinking on communities of practice in education.[1] A community of practice can be defined as:

> **Groups of people who share a concern or a passion for something they do and learn how to do it better as they interact regularly...Communities of practice are formed by people who engage in a process of collective learning in a shared domain of human endeavor.[2]**

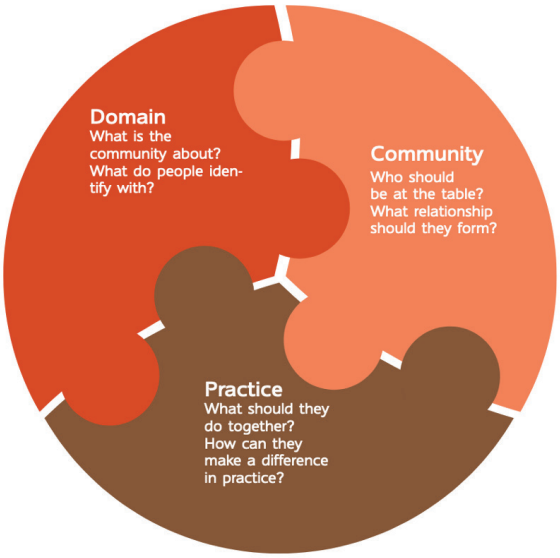

Figure 2. *Structural Elements of Communities of Practice.[3]*

[1] Wenger-Trayner E, Wenger-Trayner B, Reid P, et al. (2023) COMMUNITIES OF PRACTICE. Second Edition. Available at https://www.wenger-trayner.com/wp-content/uploads/2024/03/24-02-21-CoP-guidebook-second-edition-final-2.pdf Accessed 6th December 2024. Creative Commons license Attribution - Non-Commercial 4.0 International (CC BY-NC 4.0)

[2] Ibid p11

[3] Ibid p12

DOMAIN AND PRACTICE

In consultation with early participants, it was clear that there was huge professional and personal interest in addressing the three areas identified earlier, as subsets of the domain of cybersecurity education, namely inclusion, working with industry and innovation in the classroom. Three special interest groups (SIGs) were informally established, each with a UK and US co-chair. The identification of co-chairs readily emerged on both sides of the Atlantic, with people keen to address the challenges they had been working on for years. Terms of Reference were established followed by what Wenger-Trayner et al call a non-launch[4] of SIGs, where they state:

> **One very simple way to launch a community of practice is not to launch a community at all. Rather you convene an informal social learning space to give people an experience of learning together—and see if they want more.**

Indeed, each SIG has developed its own characteristic and momentum, ranging from regular meetings and webinars in the inclusion SIGs, to regular updates on parallel activities on industry working and innovation. Other topics, such as 'competency' have emerged as themes relevant across themes in these areas.

COMMUNITY

The first year of ICEC has been allowing the SIGs to be the vehicle for community building and relationship forming. There was an explicit desire to move beyond direct involvement in educational services, to involve employer, civil society and government. To have them at the table was essential to address the challenges of innovation, inclusion and industry relevance and employability. As such ICEC has adopted a systems perspective on the challenges of cybersecurity education.

Wrapped around this SIG activity was the development of monthly online events designed to reach across the whole network, regardless of the work done in any particular SIG. A monthly discussion on the work of the SIGs, announcements of relevant national initiatives, and other business, is held on the last Wednesday of every month. A less formal session is run on the third Wednesday of every month which is called *morning coffee-afternoon tea*, signifying different timezones and a humourous shorthand for cultural preferences. At this session, a member of the network brings an issue to the 'staff room' to share, perhaps an activity they want to tell others about, or something on which they would like to get advice.

[4] Ibid p94

Also of significance was a meeting of UK and US delegates in Portugal on Science and Technology education in the Fall of 2024. This allowed further personal interaction as well and the opportunity to jointly run a cybersecurity-focused workshop for the multi-national conference.

ENABLERS AND BARRIERS OF COLLABORATION

Perhaps the most important enabler has been a general guiding principle to keep things interesting, engaging and fun. The blending of professional relationships, friendships and collegiate working has helped establish a high degree of trust, affirm shared goals and strive for diversity of cultures in engagements. The international perspective on shared challenges has been genuinely interesting and thought provoking. However, it is essential that during the formation of ICEC the network has aimed to develop activities and plans that realise a clear set of direct and indirect benefits. This includes, but is not limited to the following through better cybersecurity education:

- **Reduction in innovation 'friction' - faster time to good idea adoption without 'reinventing wheels' or 'starting from scratch'**
- **Better risk decision making based on understanding of others**
- **Better understanding of ourselves and what our own educational system produces**
- **Better intelligence about cyber threats and their impact**
- **Identification of potential research partners**
- **A broad, global understanding of supply chains. For example, a range of multi-national companies have offices close to campuses in the UK, US and elsewhere. Different working practices come into focus in collaboration**
- **Soft power as leaders in cybersecurity - the opportunity to shape the quality of compliance and standards**
- **Potential for better establishment and harmonization of cross-border standards and regulatory compliance setting**
- **Improved cyber incident response operations through maintained trust relationships**

Keeping the general principles and benefits in mind has mitigated some of the other more obvious barriers to collaboration such as limited resources and funding. There are some less obvious limits to collaboration which need to be taken into account too. For example there are limits set by program funders which must be respected. Projects may have been established without an international budget and therefore are outside of scope of funded international activity. There are also limits regarding the degree to which policy issues of one government or another may be discussed as well as clear limits on security classifications and sensitive information.

One must also remember that international collaboration is done in the context of changing national approaches and priorities. This serves as a backdrop where countries, for example, have declared they wish to be world leaders in cybersecurity or Artificial Intelligence. One must also be alert to asymmetry in relationships where one party may feel it is giving more, or benefiting less in certain circumstances. Nevertheless, much of this is mitigated by clearly focusing on the educational practice and challenges shared by educators in their day-to-day work in service of their communities, students and institutions.

Occasionally one must be wary of the wording used in our interactions such as when it was found that the term 'Anglo-American' has a different meaning in different contexts between the UK and US. The term 'UK-US' is much more usable when signifying interaction between UK and US people. These seemingly minor issues can however take on importance in terms of inclusion, and the extent to which anything might be interpreted outside of intention or context.

ICEC: A COMMUNITY OF PRACTICE FOR CYBERSECURITY EDUCATION

"The International Cybersecurity Education Collaborative (ICEC) was founded to foster sustained UK-US collaboration, leveraging national networks like NCyTE and CSE Connect. Guided by the principles of a 'community of practice,' ICEC brings together educators and institutions committed to collective learning, resource-sharing, and advancing global cybersecurity education."

CURRENT STRATEGY

Strengthening ICEC Through Special Interest Groups, Strategic Expansion, and Global Collaboration

Three Special Interest Groups were selected to focus the emerging collaborators on something practical that they could put their hands around and provide an easy "elevator speech" response to questions regarding the worthwhile nature of investing time in ICEC. They are:

- **Innovation in the classroom**
- **inclusion in the workforce and classroom**
- **Relating to industry and understanding industry workforce needs**

Each of these SIGs have developed "National leads" around the target issue who are free to engage an ever widening circle of collaborators which in turn provides expansion potential for ICEC itself. In order to track this expansion while keeping participation light and without heavy requirements, a simply data platform has been established that permits emailing to specific subsets of ICEC members that recognize SIG interests.

Expansion targets for ICEC are fluid and always start with the identification of someone in the potential country partner willing to organize that nation's network through a tour or a joint Symposium or Conference of existing ICEC members. The strategy is aligned with the existing 5 Eyes network of government-level IC leadership, but at academic level. Paramount is the inclusion of government representatives in some manner that will differ according to national culture and established perspectives. This strategy would naturally look at Canada, Australia and New Zealand as the next participants to be inducted into the network, while not rejecting the idea of other interested nations to also join.

Finally, a convenient way to find corresponding interest in other nations is to search for international conferences where papers around the topic of workforce and international sharing of experiences can promote ICEC participation. Early examples of this strategy include the Science and Technology Education 2024 conference in Portugal, the Cybersecurity Across Disciplines conference in the US and the Cyber Security Education Ecosystem Conference in the UK.

FUTURE OPPORTUNITIES

Advancing Global Cyber Workforce Development Through Collaboration and Ecosystem Innovation

The ICEC has begun to demonstrate its value with the exchange of best practices in ecosystem creation. Educators from the UK, US, and Europe are sharing cyber workforce ecosystem practices including complex issues such as competency, workforce frameworks, diversity initiatives, and cyber-related workforce activities. Furthermore, while academia is being the catalyst, the ICEC is including a broad range of partners within the cyber workforce ecosystem including learners, employers, government, unions, private training providers, philanthropies, and trade associations. Knowing that cyber ecosystems are dynamic in nature, with distinctions based on cultural, geographic, economic, and technological factors, the ICEC is at the beginning of a development and eventual maturation.

The growing participants in ICEC have a shared vision of collaboration, one that seeks to reduce barriers and promote understanding. To date, the current strategy to move the vision forward is to link partners together and bring more expertise and resources together, all while identifying barriers. Two groups have stepped forward to facilitate this large undertaking: the National Cybersecurity Education and Training Center (NCyTE.net) from the United States, and CSE Connect (cseconnect.org) from the United Kingdom.

FUTURE OF ICEC: EXPANDING GLOBAL CYBER WORKFORCE COLLABORATION

"The ICEC is forging international partnerships to address global cybersecurity workforce challenges. With participation from the UK, US, and beyond, the collaboration aims to strengthen workforce ecosystems, align competency frameworks, and promote diversity in cybersecurity.

As ICEC grows, its focus remains on quality engagement, knowledge sharing, and harmonizing global standards to meet the evolving demands of cybersecurity."

Both NCyTE and CSE Connect are working together to expand the ICEC network, including working with entities in Portugal, Spain, Ireland, Australia, and Canada. While rapid expansion would seem to be a goal, ICEC is moving cautiously to ensure that the sharing amongst the government, academia, and industry partners is focused on the quality and quantity of cyber workforce and not on sensitive research or technologies.

The ICEC has begun to demonstrate its value with the exchange of best-practices in ecosystem creation. Educators from the UK, US, and Europe are sharing cyber workforce ecosystem practices including complex issues such a competency, workforce frameworks, diversity initiatives, and cyber related workforce activities. Furthermore, while academia is being the catalyst, the ICEC is including a broad range of partners within the cyber workforce ecosystem including learners, employers, government, unions, private training providers, philanthropies, and trade associations. Knowing that cyber ecosystems are dynamic in nature, with distinctions based on cultural, geographic, economic, and technology, the ICEC is at the beginning of a development and eventual maturation as a critical part of the international community.

Perhaps the most lasting impact of the ICEC effort may be the impact of international idea sharing on the pervasive cybersecurity workforce need dilemma which spans globally and the promise for better harmonization of standards adoption. The challenge of secure enterprises, be they government or industry rests on a global view of the problem and a global view of the workforce that can solve it. And that puts responsibility squarely on all players to engage in collaborative strategies and sharing.

“THE CHALLENGE OF SECURE ENTERPRISES, BE THEY GOVERNMENT OR INDUSTRY, RESTS ON A GLOBAL VIEW OF THE PROBLEM AND A GLOBAL VIEW OF THE WORKFORCE THAT CAN SOLVE IT.”

NCyTE CENTER

National Cybersecurity Training & Education Center

CSE CONNECT

The **National Cybersecurity Training and Education Center (NCyTE)** at Whatcom Community College, funded by the NSF, enhances U.S. cybersecurity education by supporting faculty, developing resources, and strengthening industry partnerships to build the cybersecurity workforce.

CSE Connect engages a wide range of stakeholders, both nationally and internationally. Through events, and community problem-solving initiatives, we endeavour to network the cyber education community, advocating innovation in UK cyber education.

The National Cybersecurity Training and Education Center is funded by the National Science Foundation grant #2054724.