Open Access License Notice

Cyber as a Second Language? A Challenge to Cybersecurity Education

Ben Scott
Southern Cross University
Gold Coast, Australia
ORCID: 0000-0003-3209-2184

Raina Mason
Southern Cross University
Gold Coast, Australia
ORCID: 0000-0002-1009-5520

Abstract—Cybersecurity pedagogical approaches do not address the challenges faced by students with English as an additional language (EAL). Despite EAL students representing a critical labour force for this important global and multidisciplinary industry, there lacks both research and cohesive solutions to address this issue. Via student interviews and semi-thematic analysis, this paper demonstrates that EAL cybersecurity students express challenges with aspects of cybersecurity content. Secondly, it is shown that predominant cybersecurity education bodies of knowledge and frameworks do not address challenges faced by EAL cybersecurity students.

Keywords—cybersecurity education, pedagogy, language, EAL, ESL, NESB

I. Introduction

Barriers facing students with English as an additional language (EAL) present as a significant obstacle for global education providers to engage EAL cybersecurity students. These barriers include the challenge to interpret and understand a range of learning materials [1], [2]. Concurrently, the global demand for cybersecurity education, training and skills continues to increase [3]. Previous work has encapsulated cybersecurity education and skills shortages as a lack-of-people problem, a lack-of-career information problem, and ambiguity of the meaning of cybersecurity [4]–[6]. A consistent theme in the literature remains that current educational and pedagogical approaches are falling short [7].

II. Background and Motivation

Several questions have been posited in the literature as to how cybersecurity education must address the significant presence and scalable practices of some of the world's largest companies [8]. The broad options available for the prospective cybersecurity student have also been previously discussed, such as self-directed and open-source programs, certification by both vendor (e.g., CISCO, Google, Microsoft) and vendor-neutral sources (e.g., ISC, ISACA, SANS), and traditional tertiary education sources [8]. We analyse cybersecurity education frameworks that underpin curricula globally, to investigate if they address challenges to the EAL student.

Previous research has asserted that education providers have a responsibility to support EAL students in the interpretation and understanding of technocentric terminology [9]. Sociocultural and linguistic elements were previously identified as specific challenges to this objective [10]. Yet there has been no clear research nor strategy with regards to many challenges that confront EAL cybersecurity students; a cohort that is critical to meeting the significant global shortage of cybersecurity talent [7].

A. Language Barriers and Terminology

Studies have shown that practically-driven skills are considered important candidate characteristics to employers in cybersecurity [4], [7]. The impact of terminology and jargon on learning has been investigated in several technical domains. These include application and software development [11], databases [12], programming and robotics [13], [14]. Previous work by the authors has also examined the potentially exacerbated challenge on EAL students learning technical concepts [9]. Intervention strategies illustrated in the study showed significant improvement for EAL student performance, with suggested guidelines for developing assessment for international students.

There are diverging schools of thought on the very term cyberspace [15]; or should that be 'cyber space'? Similarly for what is termed 'cybersecurity' or 'cyber security'. An etymological investigation of the word 'cyber' traces back to the term cybernetics; the combination of cybernetics and space thus providing the term cyberspace [15], [16].

Terminology is briefly discussed in Caelli (2020), with a reminder that a distinct definition of cybersecurity has been required since at least 1997. Martin and Collier (2020) discussed examples of terminological ambiguity, noting that language may present as potential barriers to successfully address the call for interdisciplinary (and multidisciplinary) solutions to cybersecurity education and workforce challenges.

Whilst terminological confusion remains, the very real issue of terminological complexity prevalent in cybersecurity education can place unnecessary additional challenges on the learner. As we further illustrate, without a cohesive pedagogical approach that recognises the EAL student and adequately addresses learning challenges, interdisciplinary and multidisciplinary pedagogical methods will continue to meet obstacles.

B. Where is the Discipline?

Interdisciplinary and multidisciplinary approaches have transcended technocentric cyber workforce models and education systems [5], [17]. EAL learners represent a critical

component of multidisciplinary workforces and the world's leading companies [8]. Calls for a multidisciplinary pedagogical approach will fall short if the challenges to EAL learners are ignored.

The distinction between interdisciplinary and multidisciplinary approaches to cybersecurity education have been extensively covered; as has the importance of people and processes from diverse backgrounds in cybersecurity to any discussion on interdisciplinary or multidisciplinary curricula approaches [17].

The lack of extant cybersecurity education frameworks that successfully meet the calls for multidisciplinary pedagogical approaches was highlighted by Henry (2017), with the need to address diverse career pathways and education levels. Absent is any specific identification to address language backgrounds of the cybersecurity learner and the associated learning challenges.

C. Cybersecurity Education Frameworks

Cybersecurity bodies of knowledge and frameworks can influence education programs and students globally [18]. Knowledge areas are an important element of these frameworks and whilst such documents identify a technocentric approach to curricula (e.g., identifying the importance of 'cyber literacy'), we demonstrate that these frameworks do not specifically address challenges to EAL cybersecurity students.

The Cybersecurity Body of Knowledge (CyBOK) project approach to knowledge area development, for example, is similar to the Software Engineering Body of Knowledge (the SWEBOK); with an acknowledgment there is no extant cybersecurity taxonomy and the education landscape remains dominated by technocentric frameworks [5]. The eight knowledge areas within the Cybersecurity Education Curriculum (CSEC) body of knowledge have previously been discussed in the literature [19]. We show a distinct lack of any consideration to the EAL cybersecurity learner in predominant education frameworks.

With the objective of formally validating knowledge, skills and abilities (KSA), several researchers have looked to predominant knowledge frameworks as reference points [3], [7]. However, the question must be asked as to how KSA outcomes can be achieved without adequately considering the language background of the learner? We analysed the body of cybersecurity knowledge and skills material to observe any evidence of addressing EAL challenges.

III. Research Questions

- RQ_1: Do students with English as an additional language express challenges with cybersecurity terminology?
- RQ_2: Do predominant cybersecurity bodies of knowledge address the education of students with English as an additional language?

IV. Methods

The methodological drive of this research is qualitative. This study does not present as a Grounded Theory (GT), though it is acknowledged that whilst all attempts are made through transcription and analysis steps to objectively present the responses from the interview component, the influence of the interaction of the researcher(s) is recognised and was noted [20].

Two parts of this study were undertaken. The first, a short interview of final year students studying cybersecurity management, was coded using thematic analysis. A semi-bibliometric and semi-thematic approach was also used for the second part of the study: a review of cybersecurity bodies of knowledge and education frameworks.

A. Interviews

The participants in the interviews were final-year undergraduate students finishing a cybersecurity management course in a regional university in Australia. All the students that completed the course answered two interview questions, at the conclusion of their final oral assessment. Students were informed that the questions were not part of their assessment nor graded, that they could be open and honest and they were encouraged to amplify their answers if they wished to do so. The questions were:

- Q_1: Did the use of cyber terminology and 'keywords' help or hinder your understanding of the concepts in this unit?
- Q_2: What do you think is the best way to introduce these cyber keywords and this terminology to make sure everything is understood?

Thematic analysis and category coding of interview transcripts is a foundational qualitative analysis technique with regards to structured and semi-structured interviews [20]. Detailed thematic analysis and category coding steps were taken as outlined below and previously used in the field of information systems research, among others [20].

The interviews were recorded, transcribed and then analysed for possible themes. A sample of transcribed interviews were read by both researchers, and possible themes were identified. Differences in understanding and clarification of themes were reached in this initial meeting. The remainder of interviews were then analysed for these themes by each researcher separately, followed by a further meeting where any differences were discussed and agreement was reached on the themes of each interview.

B. Cybersecurity Education Framework

The second part of this study was to consider the cybersecurity bodies of knowledge and frameworks that underpin curricula globally, to investigate the extent to which they address any challenges to the EAL learner.

While there is some consensus on consistently in-demand cybersecurity programs there is no established impact metric for such education frameworks and we leave this to future

work [7], [21], [22]. The varying impacts of cybersecurity education frameworks are also discussed in later sections.

Similar to the approach taken by Furnell and Bishop (2020), the surveyed items in this study were:

- Cyber Security Education Curriculum (CSEC)
- Cyber Security Body of Knowledge (CyBOK)
- $(ISC)^2$ Common Body of Knowledge (CBK)
- NICE Framework Competencies: Assessing Learners for Cybersecurity Work (NISTIR 8355)
- Workforce Framework for Cybersecurity (NICE Framework) - NIST Special Publication 800-181
- ASD Cyber Skills Framework (ASDCSF)

We conducted an analysis of these bodies of knowledge using the following themes:

- Language challenges or challenges facing EAL learners
- Terminology or jargon
- Pedagogical design
- Professional practice

C. Hypothesis

- H_1: Students with English as an additional language express challenges with cybersecurity terminology.
- H_2: The majority of predominant cybersecurity bodies of knowledge do not address the challenges expressed by EAL students regarding cybersecurity content.

V. Results

A. EAL Cybersecurity Student Interviews

A total of thirty-one (31) undergraduate students participated in the interview component. Of these, 28 were EAL international students from various non-English speaking students, and three had English as their first language. Five of the interview recordings unfortunately had technical difficulties that made them unusable, and another two interview respondents decided to discontinue after the first question was asked. Analysis was completed of the themes in the remaining 24 transcripts.

The interviews were short, necessitated by their positioning directly after the final assessment for the semester. It is therefore probably not surprising that the themes are closely related to the questions asked. The themes are shown in Table I below, along with the number of EAL and EFL students that gave answers including these themes. An example comment for each theme is below.

TABLE I. Thematic Analysis of Interviews

Theme	EAL		EFL	
	n	%	n	%
Language Barriers	2	9.5%	0	0%
Strategies to overcome language barriers	2	9.5%	0	0%
Difficulty with terminology	18	85.7%	1	33.3%
Utility of keywords	13	61.9%	2	66.7%
General difficulty with course	4	19%	0	0%

Language Barriers: “Because my English is not very good, so sometimes I would be very confused when listening to lectures, because there are often in the course of words, I don’t know ...” (Int01)

Strategies to overcome language barriers: “Actually, I had written my own list of definitions as I do this in all my subjects.” (Int13) “I often use of spare time to reading Wikipedia and translated into my own language, so that I can better understand on this course.” (Int01)

Difficulty with terminology: “Yeah. these can be a challenge to be understanding these as they can be a different function for different things. Yeah. It is best if learning these words early in course. We look at these early so it was not so hard for me. But these words can be confusing.” (Int09)

Utility of keywords: “Yes the terms help you to manage the concepts of learning. Actually this is hardest part. When using these terms of cybersecurity we need to be careful with understanding these. As so many terms are there, we must be careful we are using these in a correct way. If we do not we will be not understanding the reality of the problem to solve.” (Int14) “The keywords are important and can make difference between finding the information or being utterly lost.” (Int17)

General difficulties with course: “My challenges with all of this was time. Having many assignment tests for my subjects due in same week was too much and was tough” (Int10) “It is very hard for me with this semester as I have been affected with family with Covid. I try my best but know I did not do so good this time.” (Int15)

It is apparent that while most of these final year students expressed difficulty with jargon and keywords, they also found the terminology helpful, once they had mastered it. It is therefore concerning that far more EAL students (proportionally) expressed difficulty with the jargon required in this course and in cybersecurity generally than those who had English as their native tongue.

B. Cybersecurity Education Framework Analysis

We reviewed six predominant education frameworks for several themes. Several frameworks addressed matters of pedagogical design and professional practices, whilst a few explicitly addressed challenges of terminology and jargon. None specifically addressed language challenges for an EAL student.

1) *CSEC*: There is no acknowledgment nor reference to language barriers that EAL cybersecurity students may encounter in the CSEC. Interestingly, CSEC recommends reducing technocentric jargon [23, p.58] when cybersecurity practitioners are deployed to deliver security education and awareness campaigns; yet this very "burden" is not addressed when educating practitioners themselves [23, p.58]. Additionally, as part of the KSA strategies roadmap discussed in this document, it notes the requirement to be conversant in cybersecurity terminology [23, p.85].

2) *CyBOK*: The CyBOK is an important document that influences tertiary cybersecurity education globally. The CyBOK does clearly address that education is global. For example, the document does specifically acknowledge the global response required for a global problem [24, p.225]. Both pedagogical design and professional practice themes were also evident in the CyBOK [24, p.2].

The CyBOK also considers ambiguity in cyber terminology. For example, it cites the oft used 'Alice' and 'Bob' scenarios prevalent in cryptography. It discusses the widespread use of 'Alice' and 'Bob' to "refer to technological devices" in contrast to a CyBOK knowledge area where the terms 'Alice' and 'Bob' refer to people [24, p.51]. In this way, the CyBOK itself illustrates that the terms "are used in an effort to present ideas in a form likely to be familiar to security practitioners" but then clearly acknowledges there can be "significant difference in how these terms are used" [24, p.51]. As with all frameworks we reviewed, there is no specific consideration in the document to address challenges to the EAL cybersecurity learner [24].

3) *(ISC)² CBK*: The (ISC)² Common Body of Knowledge (CBK) is arguably the most impactful BOK on the multimillion dollar and significantly influential cybersecurity training, skills and certification industry, given that one of the most in-demand global cybersecurity certifications is entirely based on this BOK [3], [21], [22]. However, we found no evidence in the BOK, nor the specific domains of learning, that seeks to address language challenges to the EAL cybersecurity student. This is of concern as the (ISC)² CBK specifically addresses matters of pedagogical design and roles that form the skills-base of security, which ultimately underpins the suite of certifications [25].

4) *NICE Framework - NIST Special Publication 800181*: Central to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NIST SP 800-181) document is the objective to provide "a common, consistent lexicon that categorizes and describes cybersecurity work" whilst seeking to provide guidance on how to "identify, recruit, develop, and retain cybersecurity talent" [26, p.ii]. The document does address the need for "a reference taxonomy" and "common language" for cybersecurity practitioners [26, p.vi]; though like other BOKs and frameworks it does not acknowledge nor address language barriers or challenges to the EAL learner.

The framework does address challenges of terminology and jargon [26, p.vi] and themes of pedagogical design and professional practice were found [26, p.1]. The framework discusses knowledge and skills aspects of pedagogical design considerations and specifically cites Bloom's Taxonomy as a reference point for knowledge levels [26, p.5].

5) *NISTIR 8355*: The draft NISTIR 8355 is an important supplementary document to the previously reviewed NIST SP 800-181 [27]. As with the NIST SP 800-181 it does not address challenges to the EAL cybersecurity learner.

The document contains a substantial glossary that both illustrates a list of possible challenges to an EAL cybersecurity learner and represents a prime example for where our results, recommendations and future work suggestions might apply.

6) *ASD Cyber Skills Framework (ASDCSF)*: The ASD Cyber Skills Framework (ASDCSF) is a significant document in the Australian context given that the Australian Signals Directorate (ASD) is the pre-eminent cyber intelligence agency for the nation [28]. Moreover, the document is also recommended to be considered as part of international approaches, such as the NICE Framework.

The framework states that it "defines the roles, capabilities and skills that are essential to ASD's cyber missions" and that it "enables targeted recruitment of cyber specialists, provides a development pathway for current and future cyber staff, and aligns skills, knowledge and attributes with national and international industry standards" [28, p.7].

Like the previously reviewed BOKs and frameworks, we found no evidence that the ASDCSF addresses challenges facing EAL students despite the ASD placing an emphasis on recruiting EAL candidates. The framework does include themes of professional practice and pedagogical design.

VI. Discussion

From the thematic analysis of student responses, we found that *difficulty with terminology* and the *utility of keywords* were the most prevalent themes. EAL cybersecurity students also expressed the themes of *language barriers* and strategies to overcome those barriers. Among the EAL cybersecurity student cohort, it was the theme of *difficulty with terminology* shown as most prevalent. This supports H_1.

The results from the cybersecurity education BOK and framework analysis clearly demonstrate that learning challenges for EAL cybersecurity students are not addressed, despite the importance of this cohort to address skills shortages. Previous research has not addressed language

backgrounds of the cybersecurity learner and associated learning challenges.

Whilst EAL cybersecurity students represent a cohort that is critical to meeting the significant global shortage of cybersecurity talent [7] our findings show that the major education frameworks and bodies of knowledge do not sufficiently address this. Our findings support H_2. The results from the cybersecurity education BOK and framework analysis clearly demonstrate EAL cybersecurity student challenges are not addressed.

VII. Limitations and Future Work

The research was principally qualitative and the interview sample consisted of primarily EAL cybersecurity students, thus it was not possible to conduct statistically significant tests for differences between cohorts. Future work might adopt additional methods and expand participant samples.

The students were also final year students rather than students who are encountering jargon for the first time. Future participant samples will seek broader coverage of knowledge background ranges. To our knowledge, a quantified impact factor for cybersecurity education frameworks is non-existent and is an avenue for future research.

We posit that such terminological ambiguity may be systemic across cybersecurity and present significant hurdles to the EAL cybersecurity student. This requires further systematic and comprehensive research approaches. Further pedagogical research, with the explicit addition of a learner's language background, is required to investigate and validate learning challenges to the EAL cybersecurity student.

References

[1] T. Murugavel, "The Problems of Non-English Medium Engineering Students and Possible Solutions," *The Indian Review of World Literature in English*, vol. 7, no. 11, pp. 1–4, 2011.

[2] P. J. Guo, "Non-Native English Speakers Learning Computer Programming: Barriers, Desires, and Design Opportunities," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, ser. CHI '18. New York, NY, USA: Association for Computing Machinery, Apr. 2018, pp. 1–14. [Online]. Available: https://doi.org/10.1145/3173574.3173970

[3] S. Furnell and M. Bishop, "Addressing cyber security skills: the spectrum, not the silo," *Computer Fraud & Security*, vol. 2020, no. 2, pp. 6–11, Feb. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1361372320300178

[4] A. P. Henry, "Mastering the cyber security skills crisis: realigning educational outcomes to industry requirements," UNSW, Canberra, Discussion paper 4, 2017, ACCS Discussion paper. [Online]. Available: http://hdl.voced.edu.au/10707/438372

[5] A. Martin and J. Collier, "Beyond awareness: Reflections on meeting the interdisciplinary cyber skills demand," in *Cyber Security Education*. UK: Routledge, 2020, pp. 55–73, num Pages: 19.

[6] J. Slay, "Training and education for cyber security, cyber defence and cyber warfare," *United Service*, vol. 67, no. 3, pp. 24–26, 31, Sep. 2016. [Online]. Available: https://search.informit.org/doi/abs/10.3316/INFORMIT.301424020269498

[7] G. Austin, *Cyber Security Education: Principles and Policies*. UK: Routledge, Jul. 2020, google-Books-ID: LWHwDwAAQBAJ.

[8] W. J. Caelli, "History and philosophy of cyber security education," in *Cyber Security Education*. UK: Routledge, 2020, pp. 8–28, num Pages: 21.

[9] R. Mason and C. Seton, "Leveling the playing field for international students in IT courses." in *Proceedings of Australasian Computing Education Conference (ACE '21)*,. Virtual: ACM, New York, NY, USA, Feb. 2021, pp. 138–146. [Online]. Available: https://doi.org/10.1145/3441636.3442316

[10] T. Bretag, S. Horrocks, and J. Smith, "Developing classroom practices to support NESB students in information systems courses: Some preliminary findings," *International Education Journal*, vol. 3, no. 4, pp. 57–69, 2002.

[11] R. Mason, G. Cooper, B. Simon, and B. Wilks, "Using Cognitive Load Theory to select an Environment for Teaching Mobile Apps Development." in ACE, 2015, pp. 47–56.

[12] R. Mason, C. Seton, and G. Cooper, "Applying cognitive load theory to the redesign of a conventional database systems course," *Computer Science Education*, vol. 26, no. 1, pp. 68–87, Jan. 2016, publisher: Routledge. [Online]. Available: https://doi.org/10.1080/08993408.2016.1160597

[13] R. Mason, "Designing introductory programming courses: the role of cognitive load," Ph.D. dissertation, Southern Cross University, 2012, pages: xxiii, 412 pages.

[14] R. Mason and G. Cooper, "Mindstorms robots and the application of cognitive load theory in introductory programming," *Computer Science Education*, vol. 23, no. 4, pp. 296–314, Dec. 2013, publisher: Routledge. [Online]. Available: https://doi.org/10.1080/08993408.2013.847152

[15] T. W. Edgar and D. O. Manz, *Research Methods for Cyber Security*. Rockland, MA, UNITED STATES: Elsevier Science & Technology Books, 2017, google-Books-ID: aRl2DQAAQBAJ.

[16] R. Ramirez and N. Choucri, "Improving Interdisciplinary Communication With Standardized Cyber Security Terminology: A Literature Review," *IEEE Access*, vol. 4, pp. 2216–2243, 2016, conference Name: IEEE Access.

[17] J. R. Blair, A. O. Hall, and E. Sobiesk, "Educating Future Multidisciplinary Cybersecurity Teams," *Computer*, vol. 52, no. 3, pp. 58–66, Mar. 2019, conference Name: Computer.

[18] J. R. S. Blair, A. O. Hall, and E. Sobiesk, "Holistic cyber education," in *Cyber Security Education*. UK: Routledge, 2020, pp. 160–172, num Pages: 13.

[19] D. Shoemaker, A. Kohnke, and K. Sigler, "What the profession of cybersecurity needs to know and do," *The EDP Audit, Control, and Security Newsletter (EDPACS)*, vol. 59, no. 2, pp. 6–18, Feb. 2019, publisher: Taylor & Francis. [Online]. Available: https://doi.org/10.1080/07366981.2019.1565106

[20] K. Williamson, L. Given, and P. Scifleet, "Qualitative data analysis," *Research Methods: Information, Systems, and Contexts*, pp. 417–439, 2013, publisher: Tilde University Press. [Online]. Available: https://researchoutput.csu.edu.au/en/publications/qualitative-data-analysis

[21] P. Wang and H. D'Cruze, "Certifications in Cybersecurity Workforce Development: A Case Study," *International Journal of Hyperconnectivity and the Internet of Things*, vol. 3, no. 2, pp. 38–57, Jul. 2019.

[22] P. Wang and H. D'Cruze, "Cybersecurity Certification: Certified Information Systems Security Professional (CISSP)," in *16th International Conference on Information Technology-New Generations (ITNG 2019)*, ser. Advances in Intelligent Systems and Computing, S. Latifi, Ed. Cham: Springer International Publishing, 2019, pp. 69–75.

[23] J. T. F. on Cybersecurity Education, Cybersecurity Curricula 2017. New York, NY, USA: Association for Computing Machinery, 2018, oCLC: 1200516850. [Online]. Available: https://dl.acm.org/doi/book/10.1145/3184594

[24] A. Rashid, H. Chivers, G. Danezis, E. Lupu, and A. Martin, "The Cyber Security Body of Knowledge," The National Cyber Security Centre, UK, Tech. Rep. 1.1.0, Mar. 2021.

[25] "The (ISC)² CBK," The International Information System Security Certification Consortium (ISC)², Tech. Rep. [Online]. Available: https://www.isc2.org/Certifications/CBK

[26] R. Petersen, D. Santos, K. Wetzel, M. Smith, and G. Witte, "Workforce Framework for Cybersecurity (NICE Framework)," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP) 800-181 Rev. 1, Nov. 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-181/rev-1/final

[27] K. Wetzel, "NICE Framework Competencies: Assessing Learners for Cybersecurity Work," National Institute of Standards and Technology, USA, Tech. Rep., 2021. [Online]. Available: https://www.nist.gov/news-events/news/2021/03/nice-framework-competencies-assessing-learners-cybersecurity-work

[28] "ASD Cyber Skills Framework," Australian Signals Directorate (ASD), Canberra, Australia, Tech. Rep. 2.0, Sep. 2020. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/asd-cyber-skills-framework