

Securing Meaning: Language Equity in Cybersecurity Translation

Dr. Andrew J. Hurd
Assistant professor
MSIT/ MS Cybersecurity
Empire University
Saratoga Springs, NY, USA
andrew.hurd@sunyempire.edu
0009-0000-1503-8472

Dr. Gloria J. Kramer-Gordon
Assistant Professor /
Program Coordinator TESOL
Empire University
Saratoga Springs, NY, USA
gloria.kramer@sunyempire.edu
0000-0002-6637-7295

Pamela Doran
Doctoral Student, CPACC,
Digital Accessibility and
Multilingual Technology Coordinator
Empire University
Saratoga Springs, NY, USA
pamela.doran@sunyempire.edu
0009-0003-6647-8007

Abstract—As cybersecurity becomes a cornerstone of global higher education, language has emerged as an unexpected point of vulnerability. Machine translation (MT) tools, increasingly used to render cybersecurity policies into multiple languages, often distort meaning by translating technical terms literally rather than conceptually. Words like *firewall*, *phishing*, or *backdoor* lose their intent in translation, creating barriers to comprehension and leaving multilingual learners at risk of misunderstanding critical policies. This paper explores the intersection of cybersecurity vocabulary, machine translation, and language equity, drawing on examples of mistranslations and language acquisition research to demonstrate how linguistic gaps can weaken both institutional safeguards and student confidence.

We argue that cybersecurity education must treat terminology with the same precision as code, recognizing that mistranslation not only undermines clarity but also compounds anxiety for multilingual learners navigating complex technical content. To address these challenges, the paper examines strategies such as the use of back-translation, custom glossaries, Universal Design for Learning (UDL) frameworks, and emerging AI translation tools like custom ChatGPT models. Together, these approaches highlight a pathway for higher education to balance inclusion with accuracy, ensuring that policies and coursework maintain both technical rigor and accessibility. By reframing cybersecurity not only as a technical field but also as a linguistic one, this research calls for a more intentional, equity-driven approach to translation that secures both data and learning outcomes.

Keywords—*Cybersecurity education, Machine translation (MT), Multilingual learners, Universal Design for Learning (UDL), Artificial intelligence (AI) in translation, Custom ChatGPT, Higher education policy, Foreign Language Classroom Anxiety (FLCA)*

I. INTRODUCTION

Cybersecurity has become one of the defining concerns of higher education in the digital era. As institutions expand their global reach, they welcome growing numbers of multilingual learners who must navigate technical coursework, institutional policies, and evolving threats in cyberspace. While this diversity enriches academic communities, it also introduces a critical challenge: ensuring that all learners can access and understand the specialized vocabulary of cybersecurity. Unlike everyday language, cybersecurity terms are highly technical, culturally embedded, and often metaphorical, making them especially difficult to translate across languages with precision.

Machine translation (MT) tools have emerged as a convenient solution, enabling institutions to quickly provide multilingual resources. Yet, the very speed and accessibility of these tools often mask deeper risks. Literal translations of technical terms can distort meaning, diminish higher education policy clarity, and leave learners vulnerable to confusion. A “firewall” rendered as a “wall of fire,” or “phishing” reduced to simple “fishing,” shifts these concepts from digital threats to misleading images that weaken comprehension. For international students, such mistranslations compound existing barriers, from limited academic vocabulary to heightened language anxiety, and risk undermining both institutional safeguards and learner success.

This paper investigates the intersection of machine translation, cybersecurity vocabulary, and language equity in higher education. By analyzing common mistranslations and drawing from research on language acquisition and multilingual learning, we highlight the risks posed when critical policies and concepts lose accuracy in translation. More importantly, we explore strategies—including the use of custom glossaries, back-translation techniques, Universal Design for Learning (UDL), and emerging AI tools—that can make cybersecurity education both precise and inclusive. In doing so, this work argues that cybersecurity is not only a

technical field but also a linguistic one, where accuracy in language is as vital as accuracy in code.

II. CYBERSECURITY

With global mobility rising, more multilingual learners, particularly international students, are enrolling in American higher education institutions. NAFSA: The Association of International Educators [3] noted data from the National Center for Education Statistics that “nearly one million international students are enrolled in colleges and universities across the U.S., and about half are enrolled in STEM programs”. STEM stands for Science, Technology, Engineering, and Mathematics. These programs offer various learning pathways, such as computer science, which includes areas like cybersecurity. Cybersecurity has become an essential part of today’s tech and online world, acting as security against constantly changing cyber threats such as complex malware, viruses, and unusual system activity [20]. With technical threats such as cyberattacks and data fraud endangering our global economy, not only are cybersecurity programs necessary to ensure security in cyberspace, but they have also become popular among undergraduate and postgraduate college student enrollment [19], [20]. In addition, one can learn cybersecurity through courses, certifications, or hands-on practice. However, it is widely accepted that college programs are the foundation for theoretical and key concepts and the skills needed in the field [20]. Cybersecurity fluency is a critical life skill for all students and vital to the protection of an institution.

With such growth in cybersecurity and students enrolling from all over the world, these programs will need to adapt and identify ways to support curriculum that promotes language equity. This role is crucial for the ongoing growth of cybersecurity, as self-efficacy remains a significant factor in learning and retaining cybersecurity practices [25]. Several characteristics foster self-efficacy. The first of these characteristics is knowledge. Such knowledge can be achieved in a variety of ways, but vocabulary, at its core, is key to learning any language [11]. Learning cybersecurity practices is just like learning a language; you must first start with the vocabulary and then work to understand the meaning and intent of the tenets that cybersecurity provides. When learning a language, vocabulary becomes the most essential part of understanding its meaning [16]. The use of machine translation (MT) has its benefits, but it also has limitations when it comes to properly translating domain specific and technical vocabulary. There are a series of problems when it comes to translation: direct translation may not exist, there are issues with translating intent versus meaning, there may be a one-way translation problem, and the phrase might be so foreign to the target language that a proper translation may not exist [21]. Acronyms often spell out English words that can muddle translation, such as LURE (Legacy URL Reputation Evasion) and HEAT (Highly Evasive Adaptive Threats). Case sensitive glossaries become the key to accurate translation.

When translating cybersecurity phrases or words from English to Spanish, it is not always clear that the ending translation does not preserve the meaning or the intent of the English words. While learners often embrace MT for its efficiency, accessibility, and ability to facilitate quick comprehension of new vocabulary, educators remain cautious about its broader implications [12]. Some research highlights that uncritical reliance on MT can reduce students’ motivation to engage actively with language learning, possibly weaken problem-solving skills, and limit the development of personal writing styles and creativity [12]. Beyond these concerns, educators also point to inconsistent translation of quality across languages, limited recognition of cultural and contextual nuances, and inaccuracies that may distort academic content. Collectively, these challenges complicate instructors’ efforts to accurately assess student progress and uphold academic integrity. Here are a few translations of cybersecurity terminology and their possible Spanish equivalents.

III. TRANSLATION ISSUES

One of the most pressing challenges revealed in the translation table is the tendency of MT tools to default to literal renderings of cybersecurity terms. While this approach produces outputs that may look correct on the surface (intent), it often fails to capture the specialized, metaphorical, or technical meaning intended in English (meaning). For example, the term *firewall* is frequently translated as *pared de fuego* (“wall of fire”), a phrase that conjures imagery of flames rather than a digital security barrier. Similarly, *phishing* is rendered as *pesca* (“fishing”), which strips away the metaphor of identity theft and reduces the term to a recreational activity. Additionally, acronyms that spell out English words, such as Legacy URL Reputation Evasion (LURE) and Highly Evasive Adaptive Threats (HEAT), can skew meaning significantly when they are translated as words and not phrases. Therefore, it is critical to include case-sensitive terminology in a custom glossary. Such literal interpretations can create serious misunderstandings: students may fail to recognize a phishing attempt as a cybersecurity threat or misinterpret a backdoor as a physical architectural feature rather than a covert method of system intrusion.

Another issue involves overgeneralization and lack of contextual nuances. Terms such as *spoofing* or *malware* are often reduced to broad Spanish equivalents like *falsificación* (forgery) or *software malo* (bad software). These translations lose the precision required for technical accuracy and can result in vague or misleading interpretations. Acronyms such as IDS, IPS, and SIEM also pose difficulties, as their direct translations can be awkward or imprecise, while the loss of the acronym itself weakens students’ ability to recognize these terms in professional discourse. Furthermore, some terms, such as *botnet* or *rootkit*, are best retained in English, as the Spanish alternatives (*red de robots* or *kit raíz*) sound benign or even comical, masking the malicious intent behind them. Collectively, these inconsistencies highlight the dangers of

relying on machine translation without cybersecurity-specific glossaries or human oversight, as mistranslations not only obscure meaning but may also compromise learners’ ability to apply security principles effectively.

IV. MULTILINGUAL LEARNERS AND ACADEMIC LANGUAGE

Vocabulary acquisition is the foundation of language learning; therefore, for international students to succeed academically, they must first pass English competency exams such as the TOEFL or IELTS [1]. However, passing these tests does not necessarily equate to the academic language proficiency needed for advanced-level technological coursework. Adult language learners may face many challenges with limited vocabulary, such as reading, comprehension, writing, participation, and confidence. In addition, acronyms are widely used in conversation and as part of academic content. English stands as the hierarchy of technological language due to its global presence, so understanding both vocabulary and acronyms is essential for the current generation of college students [6] to be successful. In fields like cybersecurity, where specialized terminology and culturally dependent phrases are common, accurate translation is critical to ensure that multilingual learners fully grasp both the technical and contextual meaning of the content.

According to [23, p.1507], “Academic vocabulary is of critical importance in content learning and key to classroom interactions as students are engaged in learning activities using academic language”. In any given academic entity, students are required to master content-specific vocabulary, which is often technical and used less frequently compared to conversational language [5]. The Cummins (1982) framework of Basic Interpersonal Communication (BICS) accounts for approximately 10% of an English Language Learner’s (ELL)

proficiency, indicating it is a social language, which takes about 2 years to acquire. In contrast, Cognitive Academic Language Proficiency (CALP), the context-embedded or academic language, can take up to 7 years or more to develop [4], [18]. For students to be successful, both language and content need to be integrated and taught simultaneously [23]. Hence, an adult multilingual learner who has passed an entrance exam may still not be fully proficient according to the CALP timeline, adding stress and diminishing the success rate. Cybersecurity terminology and practices rapidly change, and the practices instilled are always being updated; therefore, CALP is not a great indicator for multilingual learners’ language proficiency in cybersecurity. Furthermore, as acronyms are a constant in textbooks and English conversations, [6] noted the difficulties of translating acronyms among Spanish speakers because of their diverse dialects. To help with the success of acronyms, he added visuals to support each one used in the study. Translation guides were also provided to those unfamiliar with acronym examples so they could have clarity. However, in the case of cybersecurity vocabulary, providing translation guides may not be accurate due to the multiple possible outcomes of the translation (see Table I). The importance of verifying that English proficiency plays a vital role in classroom interactions and the difference between intent versus meaning when scoring at the advanced level of English language proficiency, individuals may struggle with specialized terminology or discipline-specific dialog [1], [23]. These struggles with classroom interactions can be directly reflected in individuals who are trying to read specific policies and differentiate between intent and meaning. Higher Education policy translations targeting non-English languages present a unique scenario potentially leading to different connotations and mixed or missed instructions.

TABLE I. Sample English words and phrases translated to Spanish

Term	Common Mistranslation	Issue	Correct Term
Firewall	pared de fuego	MT often interprets it literally instead of as a network security device.	cortafuegos
Phishing	pesca or pescando	The metaphor is misunderstood as actual fishing.	suplantación de identidad or phishing (kept in English in some contexts)
Spoofing	falsificación (too general) or burlarse (mocking)	The term may be treated as a generic forgery or misinterpreted emotionally.	suplantación or spoofing (depending on the subtype, like IP spoofing)
Malware	software malo or programa malicioso (sometimes too broad)	Over-simplification or imprecise categorization.	malware (widely adopted in Spanish) or software malicioso
Brute Force Attack	ataque de fuerza bruta (literal but ambiguous without context)	While technically accurate, it’s sometimes misunderstood as a physical attack.	ataque por fuerza bruta or ataque de prueba y error
Botnet	red de robots	Overliteral and misleading; doesn’t convey the malicious intent.	botnet (accepted as-is in cybersecurity contexts)

Term	Common Mistranslation	Issue	Correct Term
Zero-Day Vulnerability	vulnerabilidad de cero días	Literal but can be confusing without explanation.	vulnerabilidad de día cero (used more idiomatically)
Rootkit	paquete raíz or kit raíz	The system may assume it's hardware or gardening tool.	rootkit (borrowed term, like malware)
Ransomware	software de rescate or secuestro de software	Literal rendering misses the nuance of extortion.	ransomware or software de secuestro (the latter is rare but sometimes used)
Backdoor	puerta trasera	Literal but misleads if context isn't clear; sounds architectural.	acceso oculto or puerta trasera (en seguridad informática)
VPN	Stands for: Virtual Private Network	Red virtual privada (literal but misses technical meaning)	Red privada virtual (RPV) – though "VPN" is often kept in practice
IDS	Stands for: Intrusion Detection System	Sistema de detección de intrusos (not wrong, but sometimes reduced to just "detección")	Sistema de detección de intrusiones
IPS	Stands for: Intrusion Prevention System	Sistema de prevención de intrusos	Sistema de prevención de intrusiones
MITM	Stands for: Man-In-The-Middle (Attack)	Hombre en el medio	Ataque de intermediario or ataque de hombre en el medio (more common)
SOC	Stands for: Security Operations Center	Centro de operaciones de seguridad (not wrong, but context often lost)	Centro de operaciones de seguridad (SOC) – acronym is often retained
SIEM	Stands for: Security Information and Event Management	Gestión de eventos e información de seguridad (reversed order, unclear)	Gestión de información y eventos de seguridad
APT	Stands for: Advanced Persistent Threat	Amenaza persistente avanzada (literal but misunderstood as something ongoing but benign)	Amenaza persistente avanzada (still used, but needs context for clarity)
CVE	Stands for: Common Vulnerabilities and Exposures	Vulnerabilidades y exposiciones comunes	Listado común de vulnerabilidades y exposiciones (still often referred to by acronym CVE)
IAM	Stands for: Identity and Access Management	Gestión de identidad y acceso (not technically wrong but sometimes flipped to acceso e identidad)	Gestión de identidades y accesos

Another obstacle multilingual learners face is known as Foreign Language Classroom Anxiety (FLCA), a type of anxiety that is triggered when confidence in speaking and writing in the non-native language is low. When academic settings rely heavily on technical jargon, communication challenges are intensified, creating significant barriers to academic success. These language barriers can lead to difficulties when individuals are required to interpret and follow translated policies while experiencing elevated levels of anxiety. Stress and anxiety may further limit individuals' cognitive access to their second language (L2), adding another layer of difficulty to comprehension and decision-making [7]. This barrier heightens the already existing anxiety; a tactic often exploited by hackers and malicious actors to secure access to individuals' personally identifiable information (PII). If a person is flustered or on edge, they are more prone to make

mistakes when dealing with cybersecurity practices [14], [17]. Previous studies on international students show that addressing and reducing anxiety fosters higher levels of engagement, leading to overall success [1]. To make learning easier and reduce anxiety, researchers recommend creating classrooms that focus on using students' language skills, cultural backgrounds, and support in their native languages [8], [9]. This support becomes essential when discussing the translations of policies and the determination between intent and meaning, as the general population leans heavily on free machine translation (MT) tools. Policies need to be mindful of the free MT tools' output, as these tools will be the first avenue of comprehension for those with low English proficiency. This is particularly important as it is not always viable to have professional translations done of existing policies. By using a back translation technique [22], Higher Education policy

authors can test the accuracy of the MT output to help, but not completely mitigate, any confusion or inaccuracies. Educators are using a variety of tools to promote vocabulary learning and retention, including “iPads, smartphones, multimedia books, native languages and computer-based learning systems” [10, p. 64]. These tools are important for those in cybersecurity programs, as reading complex texts and participating in research are essential to learning, application, and recognizing meaning [26]. By examining actual translation errors through back translation, we show how potential inaccuracies in translation can disrupt both the clarity of policies and the understanding of learners.

Reference [20] highlighted studies examining the significance of promoting inclusivity through the incorporation of Universal Design (UD) principles within course objectives. Thus, increasing collaboration among educators and expanding professional development initiatives to better support diverse learners. According to [14], the UD framework is designed to provide guidance and equitable opportunities for educators to mitigate barriers so students can participate and receive information in multiple ways without compromising content, allowing opportunities to demonstrate knowledge and skills. Reference [2] noted such an approach as flexible and accessible for all learners. Reference [24] supported students' language acquisition through social interactions and social networks by allowing them to choose their learning goals and participate within communities. Failing to address vocabulary gaps and acknowledging the rich cultural and linguistic backgrounds of students will create barriers for all multilingual learners in cybersecurity programs. Therefore, it is critical to have the MT informed by a custom glossary of terms specific to cybersecurity and the institution it serves. The glossary provides the MT with generic, context-free replacement words. It is clear that cybersecurity programs need to tailor their courses with a focus on accurate multilingual vocabulary to ensure that learners achieve the benchmarks needed to graduate. More importantly, the future of STEM programs needs to be fully prepared to engage with multilingual audiences about security software development, AI applications, and all phases of cyberspace [19].

A. Custom ChatGPT as a Support

A custom ChatGPT can make translation faster, more accurate, and more natural by adapting to the specific needs of a project or audience. It can follow industry-specific terminology, tone, and style guidelines while utilizing built-in glossaries to maintain consistent translations. By tracking context across documents or conversations, it reduces ambiguity and preserves meaning. It captures cultural nuances, whether that involves selecting the appropriate regional variation or deciding between formal and informal phrasing. Quality improves through smart checks, such as grammar reviews, consistency monitoring, and back-translation, to confirm that meaning is intact and not just intent was captured. It can also streamline work by handling bulk translations, working directly with uploaded files, and supporting human translators with polished suggestions. As it

learns from feedback, it becomes more accurate and aligned with the current writing style, resulting in each translation being smoother and more tailored than the last [15].

V. CONCLUSION

Cybersecurity depends not only on advanced technical safeguards but also on the clarity of its language. As this paper has shown, the mistranslation of cybersecurity terminology through machine translation tools poses a significant risk for multilingual learners in higher education. Literal renderings distort technical meaning, weaken institutional policies, and create barriers that increase vulnerability for students and institutions alike. The issue is not only linguistic but also pedagogical: when language equity is undermined, both comprehension and self-efficacy decline, amplifying academic stress, and the likelihood of cybersecurity errors. Addressing this problem requires intentional strategies that merge language support with technical accuracy, ensuring that cybersecurity education is accessible, precise, and inclusive for a diverse student population. The need to differentiate between intent and meaning with the output of the MT becomes essential for the target population. The accuracy of the translation will depend on the driven meaning of the corpus that is being translated. We as educators and researchers must focus on the meaning of the output to ensure that learners and constituents can adhere to the policy's intent, while striving to provide the best possible meaning.

A. Recommendations

Research of this nature is essential for MT and TESOL programs moving forward. The researchers believe that there are a few recommendations that will help institutionalize proper translations. The first recommendation is to always try to complete a back translation whenever possible to check for accuracy. Second, develop and integrate cybersecurity-specific glossaries to assist with MT and to set the standards for best practices. Institutions should create standardized multilingual glossaries tailored to cybersecurity terms, vetted by both language specialists and cybersecurity experts. Embedding these glossaries into translation workflows (including custom MT or ChatGPT tools) reduces ambiguity and ensures that meaning, not just literal words, is preserved. Third, adopt inclusive teaching and higher education policy design practices for multilingual learners. Cybersecurity programs and institutional policies must embed Universal Design (UD) principles and multilingual scaffolding into course delivery and documentation. This includes providing clear visuals, acronym guides, back-translations, and opportunities for multilingual learners to engage with content in supportive ways that reduce anxiety and enhance comprehension. Lastly, leverage custom AI translation tools with human oversight. While free MT tools fall short, custom AI models like ChatGPT, trained with domain-specific data and glossaries, offer promising improvements. However, these should be implemented alongside human oversight, faculty, instructional designers, or trained translators to validate

accuracy, monitor cultural nuance, and adapt translations to evolving cybersecurity contexts and marked with a clear identifier to show that a human presence was involved with the translation. We propose that this informational paper be used as a foundation for higher education policy creation and examination of cybersecurity terminology when translated for multilingual audiences when using machine translation. The researchers acknowledge that this study forms the basis for future research projects that implement back translations and verifications of terminology between multiple languages.

REFERENCES

- [1] Alkhalidi, S., & Bista, K. (2025). Examining language anxiety and academic success of Saudi international students in U.S. colleges. *Journal of International Students*, 15(3), 163–182.
- [2] Bray, A., Devitt, A., Banks, J., Sánchez-Fuentes, S., Sandoval, M., Riviou, K., Byrne, D., Flood, M., Reale, J., & Terrenzio, S. (2023). What next for Universal Design for Learning? A systematic literature review of technology in UDL implementations at second level. *British Journal of Educational Technology*, 00, 1–26. DOI:10.1111/bjet.13328
- [3] Brimmer, E. (2022, November 18). *International STEM talent and U.S. research competitiveness* [Blog post]. NAFSA: Association of International Educators. <https://www.nafsa.org/blog/international-stem-talent-and-us-research-competitiveness>
- [4] Bylund, J. (2011, January 1). Thought and second language: a Vygotskian framework for understanding BICS and CALP. *Communique*, 39(5), 4.
- [5] Carrier, K. A. (2005). Key issues for teaching English language learners in academic classrooms. *Middle School Journal* (J1), 37(2), 4–9.
- [6] Cedeno, P. (2025). Effectiveness of Spanish acronyms as a communication tool for the Hispanic community. *Educational Research Quarterly*, 48(3), 3–26.
- [7] Dewey, D. P., Belnap, R. K., & Steffen, P. (2018). Anxiety: Stress, Foreign Language Classroom Anxiety, and Enjoyment During Study Abroad in Amman, Jordan. *Annual Review of Applied Linguistics*, 38, 140–161. doi:10.1017/S0267190518000107
- [8] Echevarria, J., & McDonough, R. (1993). Instructional conversations in special education settings: Issues and accommodations. National Center for Research on Cultural Diversity and Second Language Learning. <https://escholarship.org/uc/item/0tq0d304>
- [9] García, S. B., & Tyler, B.-J. (2010). Meeting the needs of English language learners with learning disabilities in the general Curriculum. *Theory Into Practice*, 49(2), 113–120. <https://doi.org/10.1080/00405841003626585>
- [10] Jiang, Y., Wang, Q., & Weng, Z. (2022). The influence of technology in educating English language learners at-risk or with disabilities: A systematic review. *Center for Educational Policy Studies Journal*, 12(4), 53–74.
- [11] Johnson, M. D., Acevedo, A., & Mercado, L. (2016). Vocabulary knowledge and vocabulary use in second language writing. *TESOL Journal*, 7(3), 700-715.
- [12] Kilmova, B. (2025). Use of machine translation in foreign language education. *Cogent Arts and Humanities*, 12(1), 1-14, 2491183, <https://doi.org/10.1080/23311983.2025.2491183>
- [13] Kramer-Gordon, G. J. & Bradley, E.G. (2023). Eliminating Barriers for Non-Traditional Minority Adult Learners (NMALs) in Online Spaces. In Lyn, A. E. & Broderick M. (Eds.), *Motivation and Momentum in Adult Online Education*. IGI Global. <https://www.igi-global.com/chapter/eliminating-barriers-for-non-traditional-minority-adult-learners-nmals-in-online-spaces/322691>
- [14] Moskwa, F. J. (2024). *Exploration of the Impact of Anxiety on Cybersecurity* (Doctoral dissertation, Marymount University).
- [15] Moslem, Y., Romani, G., Molaei, M., Haque, R., Kelleher, J., & Way, A. (2023). *Domain Terminology Integration into Machine Translation: Leveraging Large Language Models* (pp. 902–911). <https://aclanthology.org/2023.wmt-1.82.pdf>
- [16] Nation, I. S. P. (2005). Teaching and learning vocabulary. In *Handbook of research in second language teaching and learning* (pp. 581-595). Routledge.
- [17] Nobles, C. (2022). Stress, burnout, and security fatigue in cybersecurity: A human factors problem. *Holistica Journal of Business and Public Administration*, 13(1), 49-72.
- [18] Roessingh, H. (2006). BICS-CALP: *An introduction for some, a review for others*. *TESL Canada Journal*, 23(2), 91–96.
- [19] Ruiz, N., Shukla, P., & Kazemian, H. (2021). Cybersecurity index for undergraduate computer science courses in the UK. *Journal of Applied Security Research*, 16(4), 456–469. <https://doi.org/10.1080/19361610.2020.1798173>
- [20] Salem, M., Samara, K., & Abdel-Karim Al-Tamimi. (2024). Navigating challenges in online cybersecurity education: Insights from postgraduate students and prospects for a standardized framework. *ACM Transactions on Computing Education*, 24(4). <https://doi.org/10.1145/3703163>
- [21] Sechrest, L., Fay, T. L., & Zaidi, S. H. (1972). Problems of translation in cross-cultural research. *Journal of cross-cultural psychology*, 3(1), 41-56.
- [22] Shigenobu, T. (2007). Evaluation and Usability of Back Translation for Intercultural Communication. *Lecture Notes in Computer Science*, 259–265. https://doi.org/10.1007/978-3-540-73289-1_31
- [23] Wei, L. (2021). Teaching academic vocabulary to English language learners (ELLs). *Theory and Practice in Language Studies*, 11(12), 1507. <https://doi.org/10.17507/tpls.1112.01>
- [24] York, J. (2023). Engaging with the world: Applying connected learning in a university language learning context. *Foreign Language Annals*, 56(2), 334–361. <https://doi.org/10.1111/flan.12691>
- [25] Zainal, N. C., Puad, M. H. M., & Sani, N. F. M. (2022). Moderating effect of self-efficacy in the relationship between knowledge, attitude and environment behavior of cybersecurity awareness. *Asian Social Science*, 18(1), 1-55.
- [26] Zhihong Xu, Kausalai Wijekumar, Qing Wang, Robin Irey, & Hua Liang. (2024). The effects of web-based text structure strategy instruction on adult Chinese ELLs' reading comprehension and reading strategy use. *Language Teaching Research*, 28(4), 1288–1310. <https://doi.org/10.1177/13621688211022308>