Open Access License Notice

Addressing the Need for Interculturality in Cybersecurity Education

Stephanie Swartz
School of Business
Mainz University of Applied Sciences
Mainz, Germany
stephanie.swartz@hs-mainz.de
0000-0003-0758-6393

Deveeshree Nayak
School of Engineering and Technology
University of Washington, Tacoma
Tacoma, WA, USA
dnayak@uw.edu
0009-0003-7819-284X

***Abstract*—This paper addresses the need for incorporating global virtual team (GVT) projects into cybersecurity education curricula in an effort to develop students' understanding of different cultures and hone their abilities to work across multiple time zones, communicate using digital communication platforms as well as improve their virtual project and time management skills. An example of a GVTs project, Virtual Business Professional, is presented in order to illustrate how collaborative online international learning (COIL) can be embedded into IT-related coursework. It is the authors' intention to encourage instructors and administrators at institutions of higher learning to support and carry out transdisciplinary GVT projects in order to best prepare graduates for the challenges of the 21st century global workplace.**

Keywords—cybersecurity education, interculturality, global virtual teams projects, collaborative online international learning (COIL)

I. INTRODUCTION

Before the Covid-19 pandemic and especially post-pandemic, institutions of higher learning have incorporated digital tools into their curricula, taking advantage of access to expertise outside the region and bringing colleagues as well as students together on collaborative projects. Through virtual learning, students benefit from exposure to professors and peers from other countries. By engaging in global virtual teams (GVT) projects using collaborative digital communication tools, students develop their skills in language, virtual intelligence, and intercultural competencies. Copious research exists on the benefits of embedding Collaborative Online International Learning (COIL) into curricula [1] [2] [3] [4]. These benefits include imparting the above-mentioned competencies in order to better prepare graduates for the digital workplace, as well as offering students international exposure, who might not ordinarily be able to go abroad due to financial, family or health constraints.

Despite the opportunities provided through virtual learning or COIL, GVT projects are often limited to interested colleagues willing to invest the time and energy, and who have developed relationships with similarly motivated colleagues through partnerships or networking. A look over the literature regarding COIL projects reveals a stronger prevalence of projects initiated in the social sciences and business disciplines [5]. Despite calls for increased digitalization across all disciplines, a large number of areas of higher learning such law, medicine and STEM are reluctant to alter their approach to education [5] [6]. The reasons are multifaceted; resistance to change, time restraints, or lack of support from department administrators might explain some reticence. However, partly to blame may be underestimating the benefits of virtual exchange, especially in the context of transdisciplinary learning.

Traditional IT coursework emphasizes primarily subject areas such as mathematics and software engineering but often neglects soft skills. This has been found to be particularly true of cybersecurity education, which is considered a purely technical discipline. Costigan refers to cybersecurity education as a "geek ghetto" [5], or an academic silo, regardless of the wide range of competencies expected of graduates of cybersecurity programs. According to experts, educators must be mindful of the kinds of jobs cybersecurity professionals enter into and thus must include social as well as transdisciplinary skills in addition to technical expertise [5].

Furthermore, virtual learning incorporated in the curricula facilitates virtual intelligence, develop students' resilience, practice-readiness, as well as frustration tolerance and empathy [6]. Essential for cybersecurity professionals are teamwork skills, which enable them to collaboratively search for solutions to cyberthreats [7]. Communication skills and the ability to interact in a team, as well as to ascertain individual team members' strengths when delegating or assigning tasks are critical to their work. These abilities include communicating across digital channels and building rapport within relatively short time periods [7]. Experiential learning through GVT projects allows students to hone these essential skills in order to best prepare for the challenges they can expect in their professional lives.

In the following paper, the authors substantiate the need for including intercultural competencies in cybersecurity education. Furthermore, we underline the relevance of GVT projects for meeting that need. Finally, we emphasize the value of engaging students from various disciplines in GVT projects. To illustrate, we describe a study involving computer science students enrolled in an Information

Systems program at a German university, who engaged in a collaborative GVT project with peers from various study programs at universities across the globe.

II. CYBERSECURITY EDUCATION

Cybersecurity education plays a vital role in preparing students for careers in cybersecurity. According to the Cybersecurity and Infrastructure Security Agency (CISA), the demand for skilled cyber professionals is very high, congruent with the increase in cyber threats. The CISA is committed to strengthening the cybersecurity workforce in the United States by establishing standardized roles that can effectively address the skills gap in the field of cybersecurity. The objective is to improve the country's preparedness against cybersecurity threats and ensure effective cyberattack responses [8].

Higher learning institutions and universities offer cybersecurity education that provides students with comprehensive knowledge, skills, and ethical principles to safeguard digital assets and combat cyber threats. These programs are available at the certificate's, associate's, bachelor's, master's, and doctoral levels, and they cover a broad range of technical subjects such as network security, data security, cryptography, digital forensics, ethical hacking, risk management, etc. The curriculum is designed to provide students with the necessary expertise to handle complex cybersecurity challenges and address cyberattacks.

Through the past decade, CYBER.ORG has developed an extensive K-12 cyber education program offering suitable content for different age groups. The Cyber.org program matches and aligns with different state education standards across the USA. This program's impact is significant and offered thousands of teachers and students with resources, training, and cyber content, which enhanced the future of the cyber workforce [9].

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is a collaboration between the Cybersecurity and Infrastructure Security Agency (CISA), National Security Agency (NSA), and Federal Bureau of Investigation (FBI) aimed at reducing vulnerabilities in the national and critical infrastructure. The program promotes cybersecurity education and expertise by designating two- and four-year institutions as National Centers of Academic Excellence in Cyber Defense (CAE-CD), Research (CAE-R), and Cyber Operations (CAE-CO) [10]. The NCAE-C program aims to develop and administer a cooperative cybersecurity education program in partnership with community colleges, colleges, and universities. The program has the following objectives: Setting cybersecurity curriculum standards and ensuring academic excellence, fostering competency development among students and faculty, emphasizing community outreach and leadership in professional development, as well as integrating cybersecurity practices across academic disciplines within the institution [11].

III. CYBERSECURITY AND CULTURE

Multiple studies confirm the relationship between cybersecurity, data protection and culture. Cross-cultural comparative studies involving the United States and European countries point to the differences in approach to privacy, individual rights to and use of personal data, as well as trust in government. For example, when comparing the Dutch to American privacy perceptions, the former were found to have fewer privacy concerns and greater trust in the government [12]. This is related back to the stringent EU General Data Protection Regulation (GDPR) passed in 2016, which allows EU citizens significant control over their personal data and requires a high degree of company compliance to regulations involving the use of data. In comparison, only a few states offer data protection and there are no federal regulations guaranteeing US citizens' rights to data privacy [12].

Drawing on Hofstede's [13] cultural dimensions, members of more collectivistic societies such as Korea tend to be more trusting while highly individualistic cultures such as the United States tend to be suspicious of regulation [14]. In addition to differences in attitudes towards privacy, there also exist disparities regarding the perception of risk and the need for risk avoidance in various cultures. For example, cultures with a high uncertainty avoidance [13], in other words adversity to risk, such as France or Germany, may place greater emphasis on good security practices and avoiding risky behavior [15]. This coincides with the characterization of "tight" and "loose" cultures, the former emphasizing the propensity for regulating social behavior while the latter focusing on individual freedoms and distaste for strictly adhering to rules [16] [17] [18].

Divergences in perception towards privacy and risk are not limited to national cultures. Studies done in the United States have found disparities among various demographics as well. In the case of gender, women were found to exhibit divergent online behavior compared to men. White males were found to be less risk averse and be less trusting of regulatory systems than both women and people of color [15] [19].

Not only attitudes towards the likelihood of risk and the importance of protecting one's data vary from culture to culture but also the understanding of what cybercrime is and how perpetrators are to be dealt with may vary depending on the cultural environment. Just as values may change depending on the culture, attitudes towards what constitutes a crime, a cybercrime or cyber-offense, as well as their social and cultural acceptability, may vary as well [20]. According to Kshetri and Alcantara [20], perpetrators may be viewed anywhere from passive acceptance to even patriotic heroes, depending on their motivations. Hackers in the United States tend to be seen as motivated by personal interests, while European or Russian hackers are often viewed as politically motivated in the interest of human rights, nationalism or, in the case of the Middle East, religion [20].

Furthermore, cybercriminals often invoke negative attitudes towards cultural "Others" when justifying the

victimization of, for example, wealthy Westerners, while sparing people from their own culture and region [20]. Cultural norms may dictate public perception in regard to how social behavior is sanctioned and offenders are persecuted [21]. To sum up, "cultural factors influence how issues around a cybercrime are constructed, and how a cybercrime is defined, conceptualized, theorized, measured, responded to and policed" [22]. The relevance of cultural factors for the nature of cybercrimes has made determining the cultural "footprint" an important element of investigations into the source of such crimes [20].

Just as cultural norms and perceptions influence the way in which individuals navigate through digital spaces, digital technology, in turn, impacts the direction in which cultural values and social behavior evolves. Algorithms, social engineering, and data collection as well as data analysis, guide people's preferences, their decision-making and even their autonomy, encouraging some norms while discarding others, partially through the implicit biases of their creators [23].

While country of origin and demographics play an important role in defining the approach to cybersecurity, nevertheless the standards developed to regulate cybersecurity are largely determined by Western countries, primarily the USA and Europe. According to Herbert et al. [24], studies underline privacy and security attitudes of Western societies as the "norm" whereas those of non-Western cultures as "exotic". Taking into consideration the cultural biases of software engineers, and policy-makers, as well as those that manage information security in regards to the perception of users, it is questionable whether a "one-size-fits-all" approach to cybersecurity can be effective in fighting a global problem [25]. "Any framework which proceeds with the misconstrual that information is value neutral, and independent of its context, will prove to be inherently problematic, unethical and insufficient" [26].

Cross-cultural research has shown that culture manifests itself in all facets of cybersecurity, beginning with the development of digital technology, including its developers as well as users, the standards with which it is regulated, and the enforcement of standards and regulations [12] [24] [21]. Cybercrime is a global phenomenon, which all countries face, and for which cybersecurity professionals must find global solutions. Therefore, it is imperative that an understanding of cultural differences in norms and perceptions regarding trust, risk avoidance, the importance of self and government regulation, as well as determination of crime and punishment of offenders be an integral part of cyber-education.

IV. GLOBAL VIRTUAL TEAM PROJECTS

A. GVT projects in IT related work

GVT project work has become standard practice for professionals working in the area of information technology. Partly responsible for this development has been the offshoring of IT jobs to India and other countries for more than a decade [27]. Projections for 2023 place ICT workers at 62 million worldwide [28]. Facilitating the rapid growth of remote and GVT project work has been the COVID-19 pandemic as well as global disruptions through war and climate change [29].

Executing projects with heterogeneous teams over multiple time zones and entirely through the use of digital communication tools and collaborative platforms presents even the most computer savvy IT professionals with multiple challenges. Apart from language barriers, interconnectivity issues and diverse work schedules, teammates face challenges of developing rapport and trust with each other. Often they are unfamiliar with the context in which their fellow teammates are operating, and attribute characteristics to their team "Other" due to intrinsic biases [30]. Norms attributed to work and free-time, adhering to deadlines, delegating tasks, giving as well as receiving feedback, and decision-making may differ across cultures [30] [31]. Lack of understanding of cultural differences and skills to bridge these differences can cause unnecessary delays, a breakdown within the team, and in worst case, failure to complete the task.

B. GVT projects at Higher Education institutions

In order to better prepare graduates for the challenges of working in GVTs, institutions of Higher Education have been incorporating GVT projects in the classroom [4]. This affords students the opportunity to learn about the challenges they may face later on in their professional lives, as well as develop a set of best practices to assist them in overcoming these challenges. By engaging in short-term projects with peers in partner universities across the globe using collaborative platforms such as Slack or MS Teams, students acquire self-efficacy in the use of communication technology, develop an understanding of cultural differences, as well as feedback, conflict resolution, and intercultural communication skills [32] [33]. Furthermore, collaborating in heterogeneous teams with students of various academic disciplines provides them exposure to different problem-solving approaches while offering an opportunity to contribute individual skill sets [34].

C. Virtual Business Professional Project

The Virtual Business Professional (VBP) project takes place in the fall and summer terms and regularly involves 17 institutions located in 10 countries (Colombia, China, Finland, France, Germany, India, Lithuania, Spain, Taiwan, and several states of the United States, ranging from New York to Hawaii) with over 500 students working in 90 heterogeneous teams. The students are enrolled in Business Communication courses led by participating instructors, and are studying a wide range of disciplines from Business Administration, Media, IT and Management, Retail, Insurance, International Business and Management to Applied Informatics, Engineering and Veterinarian Medicine. Students communicate entirely via digital communication platforms such as Slack and Zoom as well as social media. The instructors share a mutual understanding of the objectives of the GVT projects such as developing students' virtual project and time management skills, digital

communication abilities, as well as intercultural competencies. The project is embedded in course curricula, and the results of the collaborative project report make up a significant percentage of the students' final grades.

One such VBP project involved part-time students of Information Systems enrolled at a German university of applied sciences in the summer term of 2023. Over the course of six weeks, these students collaborated on a project in which they analyzed the online presence of an internationally operating company in terms of either their commitment to sustainability goals or to diversity and inclusion. Together with their teammates, they collected their findings and made recommendations in a final business report, which was evaluated by an international team of instructors. The top three reports were selected by a strategic advisory and consultancy agency that specializes in gender, race, workplace culture, and belonging. Participating students received microcredentials in the form of a certificate as well as a digital badge.

Upon completion of the project, 21 students answered a short, anonymous survey in which they responded to questions regarding the challenges as well as the benefits of engaging in the VBP project. The majority had never participated in a GVT project before. The greatest challenge was seen as working across different time zones and conflicting schedules. Students considered the benefits to include improving virtual teamwork skills and learning how to work with people from other cultures. A large number of students agreed that GVT projects should be an integral part of IT-related study programs. Their reasoning included the ever-increasing reliance on remote work and the international nature of IT work.

V. CONCLUSION

With the rapid development of technologies, also referred to as the Fourth Industrial Revolution, including the advancement of Artificial Intelligence (AI), countries are facing both a closer dependency upon each other as well as increased security threats [35] [36]. The rise in breaches of personal data and disruptions to businesses has meant an increasing need for cybersecurity professionals. Institutions of higher learning are required to best prepare their graduates for careers in IT-security, cybersecurity and risk management, and this involves a transdisciplinary approach, bringing the areas of IT, Law but also Management, Social Sciences and Humanities together. One such method includes engaging students in collaborative GVT projects such as the VBP where they hone their virtual project management as well as digital communication skills, and develop their understanding of working across cultural differences. Through increasing students' intercultural competencies, we can potentially reduce the risk of bias in the development and use of these technologies. At the same time, we encourage successful international collaboration and by doing so, increase the likelihood of global progress. Further research focuses on specific kinds of projects and how they develop the skills cybersecurity professionals need to meet 21st century challenges.

REFERENCES

[1] B. Barbosa, S. Swartz, C. Prado-Mezad, and Crawford, I., "Learning how to work in multicultural teams: students' insights on internationalization-at-home activities," Interpersona, vol. 13, pp. 205-219, doi: 10.5964/ijpr.v13i2.378. 2019.

[2] B. Barnowska, and M. Kozaryn, "Benefits from the implementation of project tasks with the use of virtual team," Management, vol. 22 No. 2, pp. 204-216. 2018

[3] M. Duvall, A. Matranga, and J. Silverman, "Designing for and facilitating knowledge-building Discourse in online courses. Information and Learning Sciences," vol. 121(7/8), pp. 487–501. https://doi.org/10.1108/ILS-04-2020-0081. 2020.

[4] S. Swartz, B. Barbosa, I. Crawford, and S. Luck (Eds.), Developments in Virtual Learning Environments and the Global Workplace. IGI Global. June 2021. https://doi.org/10.4018/978-1-7998-7331-0.

[5] S. S. Costigan, Shifting the Boundaries: Conceptual and Practical Challenges of Cybersecurity Education, Definitions and Expectations. University of Portsmouth. 2023.

[6] A. M. Singh, "From crisis springs opportunity: Using virtual learning to develop more effective lawyers," vol. 65 St. Louis U. L.J. (2021). https://scholarship.law.slu.edu/lj/vol65/iss3/12/.

[7] S. Chang, K. Yoon, S. Wuthie, and K. Zhang, "Capture the flag for team construction in cybersecurity," arXiv:2206.08971v1 [cs.CY] University of Colorado. 2022.

[8] Cybersecurity & Infrastructure Security Agency. 2023. https://www.cisa.gov/topics/cybersecurity-best-practices/cybersecurity-education-career-development

[9] Cyber.Org. The Academic Initiative of the Cyber Innovation Center. 2023. https://cyber.org/about-us/our-impact

[10] National Security Agency/Central Security Service. 2023. https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/

[11] Center of Academic Excellence in Cybersecurity Community. 2023. https://www.caecommunity.org/

[12] J. Vitak, Y. Liao, A. Mols, D. Trotter, M. Zimmer, P. C. Kumar, and J. Pridmore, "When do data collection and use become a matter of concern? A cross-cultural comparison of U.S. and Dutch privacy attitudes," International Journal of Communication, vol. 17 (2023), pp. 471–498 1932–8036/20230005. https://ijoc.org/index.php/ijoc/article/view/19391.

[13] G. Hofstede, J. H. Hofstede, and M. Minkov, M., Cultures and Organizations - Software of the Mind: Intercultural Cooperation and Its Importance For Survival. 2010. McGraw-Hill Education Ltd

[14] A. Hovav, and J. D'Arcy, "Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the U.S. and South Korea," Information & Management, vol. 49, Issue 2, pp. 99-110, 2012. https://doi.org/10.1016/j.im.2011.12.005.

[15] T. Halevi, N. Memon, J. Levis, P. Kumaraguru, S. Arora, N. Dagar, F. I. Alou, and J. Chen, "Cultural and psychological factors in cyber-security" November 2016 DOI: 10.1145/3011141.3011165 Conference: 18th ACM International Conference on Information Integration and Web-based Applications & Services (iiWAS) At: Singapore.

[16] E. Stamkou, G. A. van Kleef, A. C. Homan, and I-C. Lee, "Cultural collectivism and tightness moderate responses to norm violators: Effects on power perception, moral emotions, and leader support." Personality and Social Psychology Bulletin, vol 45(6):014616721880283 2018. DOI: 10.1177/0146167218802832

[17] X. Pan, D. Nau, and M. Gelfand, "Cooperative norms and the growth of threat: Differences across tight and loose cultures," 2020 7th International Conference on Behavioural and Social Computing (BESC), 2020, pp. 1-6, doi: 10.1109/BESC51023.2020.9348297. https://ieeexplore.ieee.org/document/9348297

[18] M. J. Gelfand, Rule Makers, Rule Breakers. Tight and Loose Cultures and the Secret Signals that Direct Our Lives. 2018. Little, Brown Book Group

[19] M. L. Finucane, P. Slovic, C. K. Mertz, J. Flynn, and T. A. Satterfield, "Gender, race, and perceived risk: The 'white male' effect," Health Risk & Society, vol. 2(2), pp. 159-172, 2000. DOI: 10.1080/713670162

[20] N. Kshetri, and L. L. Alcantara, Cyber-Threats and Cybersecurity Challenges: A Cross-Cultural Perspective, Nigel Holden, Snejina Michailova and Susanne Tietze (Eds) The Routledge Companion to Cross-Cultural Management, London and New York: Routledge. 2015.

[21] K. Eriksson, P. Strimling, M. Gelfand, J. Wu, Abernathy, C. S. Akotia, A. Aldashev, P. A. Andersson, G. Andrighetto, A. Anum, G. Arikan, Z. Aycan, F. Bagherian, D. Barrera, D. Basnight-Brown, and B. Batkeyev, "Perceptions of the appropriate response to norm violation in 57 societies," Nature Communications, vol. 12 p. 1481, 2021. https://doi.org/10.1038/s41467-021-21602-9

[22] H. H. Brownstein, "The social production of crime statistics, Justice Research and Policy," vol. 2, pp. 73–89. 2000.

[23] A. Brantly, "Utopia lost – Human rights in a digital world," ACIG, vol. 1, no. 1, 2022, DOI: 10.5604/01.3001.0016.1238

[24] F. Herbert , S. Becker, L. Schaewitz, J. Hielscher, M. Kowalewski, M. A. Sasse, Y. Acar, and M. Dürmuth, "A world full of privacy and security (mis)conceptions? Findings of a representative survey in 12 countries," arXiv:2212.10382v2 [cs.CR] 22 Dec 2022

[25] H. Cho, M. Metzger, S. Trepte, and E. Nekmat, "A cross-country study of comparative optimism about privacy risks on social media," International Journal of Communication, vol. 17(2023), 2003–2023 1932–8036/20230005. https://ijoc.org/index.php/ijoc/article/view/19990.

[26] A. Gautam, and D. Singh, "Building bridges: Eurocentric to intercultural information ethics," Journal of Contemporary Eastern Asia. vol. 20, No. 1, pp. 151-168. 2021. DOI: 10.17477/jcea.2021.20.1.151

[27] S. Sarkar, "U.S. offshoring of jobs and businesses to India: A survey and analysis," International Business & Economics Research Journal (IBER), vol. 5(7). 2011. DOI: 10.19030/iber.v5i7.3491

[28] Statista, 2021, https://www.statista.com/

[29] J. M. Barrero, N. Bloom, and S. J. Davis, "Working from home is the trend of the year—And next year too." Time, December 2022.

[30] T. S. Hollema, Virtual Teams Across Cultures. Create Successful Teams Around The World. 2020. Interact Global, Netherlands

[31] E. Meyer, The Culture Map: Decoding How People Think, Lead, and Get Things Done Across Cultures. 2016. PublicAffairs

[32] M. Logemann, J. Aritz, P. Cardon, S. Swartz, T. Elhaddaoui, K. Getchell, C. Fleischmann, R. Helens-Hart, X. Li, J. C. Palmer-Silveira, M. Ruiz-Garrido, S. Springer, and J. Stapp, "Standing strong amid a pandemic: How a global online team project stands up to the public health crisis," British Journal of Educational Technology, vol. 00, pp. 1-6. 2022. DOI: 10.1111/bjet.13189

[33] S. Swartz, B. Barbosa, and I. Crawford, "Building intercultural competence through virtual team collaboration across global classrooms," Business and Professional Communication Quarterly, pp. 1-23. October 2019. https://doi.org/10.1177/2329490619878834

[34] S. Swartz, and A. Shrivastava, "Stepping up the game– meeting the needs of global business through virtual team projects," Higher Education, Skills and Work-Based Learning, vol.12 (2), pp. 346-368. 2021. https://doi.org/10.1108/HESWBL-02-2021-0037

[35] M. Alawida, S. Mejri, A. Mehmood, B. Chikhaoui, and O. Isaac Abiodun, "A comprehensive study of ChatGPT: Advancements, limitations, and ethical considerations in natural language processing and cybersecurity," Information 2023, 14, p. 462. https://doi.org/10.3390/info14080462

[36] K. Schwab, "The Fourth Industrial Revolution: what it means, how to respond," World Economic Forum. 2016. https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/