Immersive Cyber-Verse: The State of Immersive Learning Techniques in Cybersecurity Education in Small Colleges

Sayonnha Mandal
Metro State University, USA

Sayonnha.mandal@metrostate.edu

Abstract: In our current predicament of alarming rise of cyberattacks, social engineering attempts and an evolving need for encrypted security, the importance of cybersecurity education and training cannot be overstated. The need to equip the current and future generation of students with all the necessary tools, knowledge and expertise to combat this ever-increasing threat is paramount. Big institutions, including R1, 2 and 3 universities have already been striving to train a cybersecurity-trained workforce and providing substantial resources and funds to continue research and exploration of this area. On the other hand, smaller institutions, including private liberal arts colleges, four-year universities and various urban colleges are often grappling with the obstacles of limited funds and the inability of utilizing expensive infrastructure to continue research in niche cybersecurity topics, such as quantum information systems, critical infrastructure systems, etc. This paper provides an overview of the various challenges faced by these smaller institutions in terms of resources for their students for the required cybersecurity training and discusses potential teaching techniques using immersive learning methods of augmented reality (AR) and virtual reality (VR). The use of these technologies is already being prevalent in imparting student learning in complex and inter-disciplinary cybersecurity topics. This paper aims to identify the challenges associated with the utilization of these technology in smaller higher learning institutions. It further discusses potential strategies to overcome these shortcomings to eventually help these universities to proactively join the commitment of building a cybersecure workforce.

Keywords: Immersive techniques, Cybersecurity education, Small colleges, Virtual reality, Augmented reality

1. Introduction

As cybersecurity techniques and applications are increasingly expanding and becoming more complex, a robust curriculum with effective and innovative teaching methods are also necessary to provide the required training to cybersecurity practitioners. Regular curriculum and content often become ineffective or stagnant in imparting the knowledge in an effective hands-on manner. On the other hand, both traditional and online learning face the challenge of engaging student interest and attention in complex subjects. The socially distant structure of remote education also decreases the feeling of connectedness with the content. Immersive technologies, blending a digitally generated environment with real world objects, allow a sense of immersion and interactivity for users, while also reducing external distractions effectively. Immersive learning has been proven to significantly improve knowledge acquisition and understanding, concept retention, and improving understanding of abstract and complex topics (Childs et. al, 2023) Moreover, for imparting more complex material, virtual reality-based techniques have been shown to increase student attention and motivation in a positive manner. Although these technologies have been used in a cybersecurity curriculum in a limited manner, we focus on the utilization of immersive learning experiences for more targeted teaching of complex topics in cybersecurity.

Niche cybersecurity topics, such as Quantum Key Distribution, Post-quantum Cryptography, SCADA systems security, etc. are often not included as part of the regular curriculum taught in smaller institutions due to various constraints. We explore the use of virtual reality technologies (termed “CyberVerse”), as a potential method of teaching these cybersecurity topics to attract and retain student interest as well as render complex knowledge in a user-friendly manner. In this paper, we therefore address the following research question:

What are the key barriers to adopting immersive learning technologies for teaching niche cybersecurity topics in resource-constrained institutions, and what strategies can enable effective implementation despite limited funding and infrastructure?

We attempt to investigate this by following the steps below:

1. Investigate virtual reality usage in current cybersecurity topics
2. Identify niche cybersecurity topics which may benefit from virtual reality technologies
3. Identify limitations in smaller higher learning institutions in implementing new cybersecurity curriculum using virtual reality tools
4. Propose a four-fold method to address these constraints and build a way to develop virtual reality-based content for niche cybersecurity topics

This research thereby addresses a critical equity issue in cybersecurity education, ensuring that students at all types of higher learning institutions, have access to cutting-edge training methods necessary to combat the evolving cyber threat landscape. It strives to identify the resource gap and its impact on the development of a robust cybersecurity workforce and expand pedagogical understanding of how immersive learning addresses complex cybersecurity concepts. The rest of the paper is arranged as follows. Section 2 highlights the relevant research on virtual reality techniques, especially in cybersecurity education. Section 3 provides a deep dive into the different available virtual reality and immersive technologies. Section 4 outlines the challenges of adopting these systems. Section 5 describes our proposed implementation techniques in smaller higher learning institutions and finally Section 6 concludes our paper.

2. Related Research

M. Bruner, D. Chakravorty, N. Gober, D. McMullen, A. Payne, and J. Seo (Bruner, 2019) used physical security aspects integrated within a cybersecurity training program application. Named the Cyberinfrastructure Security Education for Professionals and Students (CiSE-Pros), focused on physical security best practices, such as, entrance requirements for data centers, secure interaction with hardware infrastructure, etc. The application also highlighted secure practices of access control, physical documents and clean desk policies.

K. Kullman, M. Ryan, and L. Trossbach (Kullman, Ryan, Trossbach, 2019) developed VRDAE (Virtual Reality Data Analysis Environment), which provided a collaborative environment and data visualization tools for network connections to train cybersecurity analysts within an enterprise environment. Moreover, two associated integrated applications named VIDS (Visual Intrusion Detection System), and VDE (Virtual Data Explorer) enabled users to participate in the secure design and implementation of network topology and traffic and security alerts, thereby exposing the users to data interaction within a virtual environment.

J. Ingalls (Ingalls, 2021) utilized mixed reality interfaces based on metadata from network appliances that allowed analysis capability for cybersecurity risk and operations. The tool, named Viewpoint, enabled collecting data from multiple sources to create an enterprise network traffic simulation. Additional activities like simulations of attack maps, intrusion models, remediate breaches and attack signature simulation were also provided for the users to interact within the environment.

P. Wagner (Wagner, 2023) developed the Virtual Exploit Network Offense Management (VENOM) tool, which enabled top networking protocols for a medium size shipping/delivery company network, to be simulated in the virtual environment. The tool also included network attack scenarios to visualize real-time network attack simulations, hence improving Security Operations Center (SOC). Situational awareness was also facilitated via the tool by integrating dashboards and visual heads-up displays in the operational environment.

Skorenkyy, Kozak, Zagorodna, Kramar, and Baran (Skorenkyy, et. al, 2021) focused on augmented reality by developing a model to map AR-assisted scenarios onto the NICE framework cybersecurity topic blocks. This tool targeted robust content development and improved user engagement for a cybersecurity training project encompassing the functional requirements, such as cybernetic, applications, services, security, interoperability, predictability and sustainability of cyber-physical systems.

Scholefield and Shepherd in their paper (Scholefield, Shepherd, 2019) performed a study that used gamification to teach password security to users. This research targeted the limitations of previous research, where gamification was mostly targeted for younger audience, especially high school students. The authors also recognized that these gamification models were primarily browser-based applications and hence had limited reach due to many having inaccessible browsers. Their postulated platform thus designed a unity role-playing quiz application for Android. The results from this application yielded positive results in improving understanding of password security concepts and accepted gamification as an effective teaching tool for cybersecurity education.

Alqahtani and Kavakli-Thorne improved upon the role-playing gaming concept by developing a CybAR, an Augmented Reality game for Cybersecurity Awareness (Alqahtani, Kavakli-Thorne, 2020). They targeted a more experienced audience set and included activities in spoofing attacks, phishing, ransomware and phone scams. Elements of both Technology Threat Avoidance Theory (TTAT) and the Persuasion Knowledge Model (Conde-pumpido) were adopted in their game framework design. This game design also produced positive results, where participants were observed to have improved cybersecurity understanding, elevated engagement with the game-based learning and increased interest in cybersecurity learning in the future.

Veneruso, Ferro, Marrella, Mecella, and Catarci observed the effectiveness of a Virtual Reality (VR) experience called CyberVR (Veneruso et. al, 2020). In this gaming mode, users were immersed in a VR avatar as an IT technician. They were then required to complete certain mini games within the platform that covered relevant cybersecurity topics. Built as a two-level game, the first level focused on building and refreshing fundamental concepts for a novice cybersecurity user. The second level then emphasized more critical real-world concepts such as network mapping/scanning, information flow, code injection, patch management, dynamic software analysis, privilege escalation, and public-key cryptography. Their experiment successfully provided positive outcomes that determined that gamified cybersecurity learning was more engaging than traditional textbook instruction and can be an effective tool to teach complex topics in the same.

Although the research and adoption of VR/AR technologies for cybersecurity are still somewhat limited, leveraging gamification strategies for teaching cybersecurity concepts remain an effective and desirable method for future content development.

3. Types of Virtual Reality Technologies

Virtual Reality consists of an absorbing, interactive, computer-mediated experience in which a person perceives a synthetic environment via specialized human-computer interface (HCI) equipment (Mandal, 2013).

Virtual reality technologies include both software and hardware components for its operability and human-computer interaction capability (Li, Zhu, 2021).

Software

- Builds interactive environment for users
- Has 3D modeling capability
- Engine capable of building the virtual environment

Hardware

- Allows data and real-world information input
- Enables injecting and receiving feedback into/from the virtual environment

Typical interactions with virtual reality interfaces so far have been using some form of controllers either controlled by a pointer or hand gestures. With advanced technology, users are now capable of virtual reality interaction in a varied number of ways. Technologies such as eye-tracking, optical body tracking, gloves, optical hand gestures, muscular/spatial, neural interfaces, and various haptic and sensory feedback devices, enable the users to completely immerse themselves in the virtual environment and affords a more seamless interface steeped in realism.

Virtual Reality experiences provided to users are categorized into the following main types (Wagner, 2023):

- Virtual Reality (VR) – Users are completely immersed in a computer-generated reality.
- Augmented Reality (AR) – enhances the real world with images, text, and other virtual information via devices such as head-up displays, smartphones, tablets, smart lenses, and glasses.
- Mixed Reality (MR) – more advanced than augmented reality enabling users to interact with virtual objects that are placed in the real world.
- Extended Reality (XR) – an all-encompassing term depicting all current and future (yet-to-be-created) immersive technologies (Marr, 2019)

Cooper and Thong (Cooper, Thong, 2019) were proponents of educational applications of virtual reality and introduced the VR Education model or VEM. The authors demonstrated the usability of VEM on 4 criteria:

- *Experience* – A learner can experience concepts of different locations such as space or phenomena such as historical times or locations, not only from their individual point of view, but also from another learner.
- *Engagement* – Measures a learner's attention novelty, interest, feedback, and challenge across the spectrum of emotional, sensory, and spatiotemporal criteria.
- *Equitability* – Promotes learning experience consistency irrespective of varied geographical locations, technology access, social and economic biases
- *Everywhere* – Denotes the ability of VR to provide CVEs or Collaborative Learning Environments to learners to promote global collaboration, unrestricted by location, time and modalities.

For the purposes of this paper, we are only going to be focusing on currently available VR and AR technologies only. Although a detailed explanation of Virtual Reality interaction is outside the scope of the paper, it is important to understand the current and future possibilities. From this point in the paper the implementation of one or both types of virtual reality technology are collectively going to be referred to as the CyberVerse.

4. Limitations of Cyber-verse Application

4.1 Traditional Challenges for VR/AR Adoption

Although VR/AR and similar technologies have been in use for several years, there have been considerable obstacles to its adoption in varied areas due to certain negative associations with the same. Specifically in areas of education, training, operational usage and teaching for younger audiences on a regular basis, this technology faces a lot of adoption barriers. Some of these issues include:

- Financial constraints due to relevant infrastructure needs
- Absence of realism in environments and fidelity
- Issues in translating and validating knowledge earned through these methods
- Physical and Psychological effects on users
- Lack of Guidance on associated curriculum development
- Need for mobile device usage by minor participants

Neelakantan (2019) explored these barriers in the context of three educational settings – K-12 schools, higher educational institutions and organizational trainings. Notably, K-12 schools were found to be faced primarily with budget constraints, lack of understanding of VR benefits, value on education and learning, retention effectiveness for students, as well as parents and guardian concerns (Neelakantan, 2019).

Matsika and Zhou (2021) in their paper explored similar concerns of VR adoption in higher educational settings and categorized them in distinct concern areas of individual security, environmental cocnerns, ethical concerns and content availability (Matsika, Zhou, 2021).

The detailed table illustrating the barriers to VR adoption in educational settings based on both Neelakantan and Matsika et. al. classifications, is below.

4.2 Adoption Challenges for Smaller Institutions

For the purposes of this paper, we define small colleges as any US institution catering to less than 5000 students, usually with a strong undergraduate focus. These institutions usually house with fewer academic programs and provide limited class sizes, but often with more personalized faculty interaction. For the scope of this paper, we are including the following types of US higher education institutions under our umbrella term of “Small colleges”:

- Private Liberal Arts Colleges
- Regional Public Colleges
- Private Non-profit Colleges

- Religious and Minority Centric Colleges

As mentioned above, all these types of higher learning institutions hold small class sizes, limited course offerings and cater to a much lower number of total students as compared to Research centric (R1 and R2) and State aided colleges in similar locations and topics. The student base also widely varies in these colleges, which often dictates course offerings and new course development. Considering these differences, we highlight the top three (technical and framework aspects combined) critical distinct challenge areas, encountered by small colleges regarding providing a comprehensive cybersecurity education utilizing virtual reality technology (Figure 1).

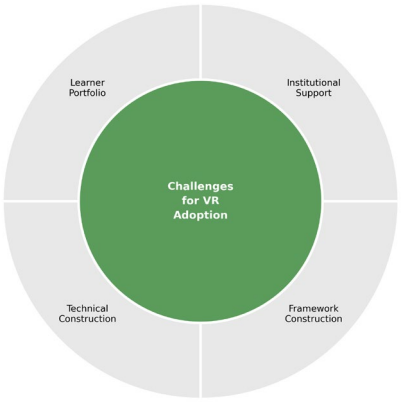

Figure 1: Challenges for CyberVerse adoption in Small Colleges

- **Learner Portfolio:** The overall student population in small colleges are mostly less than R1 and R2s. Moreover, many programs in the former, provide primarily undergraduate curriculum with no graduate degree support. Thus, the necessary background and/or experience of students to pursue specialized cybersecurity topics are very much limited. Much of the cybersecurity curriculum in small colleges is focused on enhancing application-based and technical skills for students, rather than being research or theory oriented. While many institutions do offer a combination of both aspects, students are usually on a fixed career path and a highly job centric goal, which can limit student awareness regarding niche cybersecurity topics. However, even with awareness of such topics, students are often unwilling to follow a more research-based study plan to explore these areas. Learning new concepts with perceived less employability and topic visibility is mostly the main deterrent for students to adopt a virtual reality-based approach to learn niche cybersecurity topics.
- **Institutional Support:** With the adoption and widespread utilization of any new technology and curriculum tools, small colleges need, not just departmental support, but recommendations from higher administrative levels as well. Many of the curriculum change decisions affect other related departments as well and many students with different majors/minors than cybersecurity face challenges with advanced technology usage in courses. Thus, institutions are very often reluctant to adopt new or experimental curriculum changes due to adverse issues of retention, engagement and future enrollment. Departmental faculty and staff can also be hesitant to change their course structure and introduce further challenges to student learning in the topics. Lack of managerial and collegial support may contribute to delayed or absent adoption of a newer virtual reality technology-based curriculum.
- **Technical and Framework Construction:** Finally, the financial and budget related concerns (considered together) while launching virtual reality-based curriculum is a significant limiting factor when it comes to small colleges. With limited budget allocations, usually dependent on tuition rates and private endowments and minimal or absent state and government support, adopting a virtual reality-based teaching curriculum is an ongoing challenge in smaller institutions. Acquisition, Operation, Troubleshooting and Maintenance, all require significant financial commitments from the upper management and the department, thereby posing a major obstacle in the adoption of these technology in these scenarios.

5. Proposed CyberVerse Implementation Design in Smaller Institutions

In this section, we propose several potential techniques to introduce CyberVerse in small colleges for teaching cybersecurity concepts. We look at a four-fold method to overcome the major limitations of such implementation and tailor these recommendations to be applicable to the limited infrastructure and financial resources available in these institutions (Figure 2).

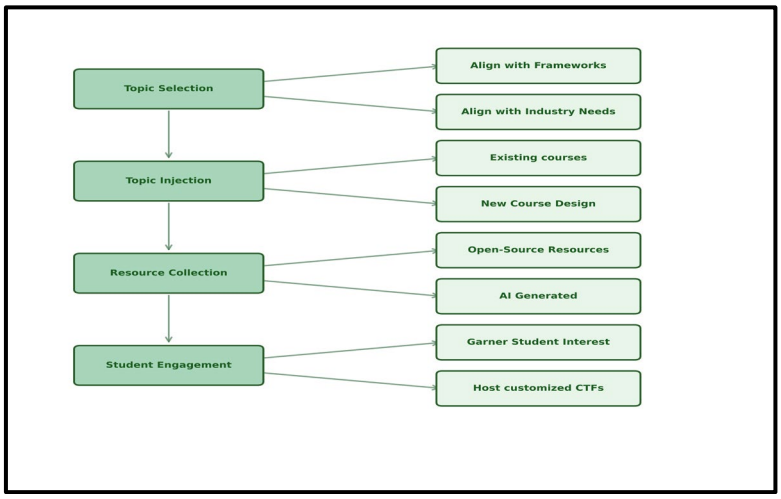

Figure 2: Process of CyberVerse implementation in Cybersecurity Education

- **Topic Selection:** Keeping in mind the allocation of limited resources in small colleges, it is a good idea to purposefully choose the topic areas in cybersecurity that can benefit students the most. Careful selection of niche but relevant cybersecurity topics can not only help retain student engagement but can also make them better prepared for future job prospects in those areas. Selecting topics in this criterion can be an overlap of required knowledge units based on frameworks for cybersecurity higher learning and current industry needs and standards in the field.

Widely adopted frameworks such as NICE and CAE are a good starting point to identify niche cybersecurity topics for this purpose. Some possible topics include:

- Cyber-Physical Systems (CPS)
- Industrial Control Systems (ICS)
- Threat Intelligence (THI)
- Offensive/defensive Cyber Operations
- Critical Infrastructure Security
- Human Factors in Information Security
- Post Quantum Cryptography
- Quantum Computing and Security

Relevant industry standards, such as ISACA and SentinelOne, include the following niche topics:

- Post-Quantum Cryptography (PQC)
- Operational Technology (OT) & IoT Security
- Identity-First Security & Decentralized Identity
- API and Serverless Security
- Zero-Trust Architecture
- Quantum Computing Threats
- Social Engineering via Deepfakes
- **Topic Injection:** Once we have identified the topics that fit into the requirements of the institution, the next step is to plan the implementation of the topics. This can be done by either integrating smaller modules in already existing courses in the department or by developing entirely new cybersecurity courses based completely on virtual reality technology. Depending on infrastructure support, student needs and instructional capabilities, a good rule-of-thumb is to slowly but deliberately introduce students to the usage of virtual reality technology learning in the new topic areas by incorporating mini modules, assignments and labs within the existing cybersecurity courses.

This gives students an exposure to the newer topics and the technology and eases the adoption and transition into this different form of learning. In instances where current course integration is not possible, designing entirely new courses with the new topics and using VR techniques to demonstrate concepts and undergo lab-based training, can be an alternate means of action. In both cases, adoption, understanding and acceptance of the different teaching method and topic choices must be slow, persistent and consistent to yield long term results. Aligning course learning outcomes with (Kirschner, 2002) can be a best practice technique in this case.

- **Resource Collection:** The next step in this four-fold process will be to obtain relevant resources for implementing these courses. Since one of the challenges faced by small colleges is the lack of financial and administrative support, we must tackle this resource gathering stage in the most efficient and cost-effective way as possible. One method is to use Open-source resources available from various R1 institutions. Several research-based VR tools are freely available from these institutions. Many organizations also market their beta version software and tools in this area as well. Some of the related research, such as CyberVR, CybAR, etc. are good examples of these. Many other open-source tools for specific topic areas are also available. For example, for quantum computing and quantum cryptography, the user-friendly simulation platform QuantumFlyTrap (https://quantumflytrap.com/virtual-lab/) and the comprehensive project lists at the Quantum Open Source Foundation are useful resources (https://qosf.org/project_list/). If open sources resources are still insufficient to meet the course needs, using the various Generative AI tools are also a fast and effective way to generate virtual reality simulations tailored to specific courses. For instance, Claude AI produced the following quick simulation of BB84 protocol with a preliminary prompt within a few minutes Figure 3). It also provided a detailed explanation of the design and implementation process and the source code to further modify the simulator as needed. Please refer to the publicly available demo (https://claude.ai/public/artifacts/bb2855d7-6584-47ab-b5dd-c34d727fd78e) and detailed information on this on my GitHub page (https://github.com/smandal-metrostate/BB84-VR). Using more targeted prompts with similar GenAI tools can also be a useful way to produce real-world models for students to practice their cybersecurity skills in the selected topic areas.

Figure 3: BB84 protocol simulation generated by Claude AI

- **Student Interest:** The final step in the CyberVerse implementation in small colleges is cultivating and maintaining student engagement and course retention. Since the selected niche cybersecurity topics maybe less popular or even unknown to many novice cybersecurity students, it is important to garner attention and visibility to the same. Ways to do that can include increased marketing on these topics through advising, student club events, class auditing, and offering special topics courses. Creating awareness and maintaining relevance to the CyberVerse implementation can also be done by hosting occasional in-house CyberVerse CTFs, local high school CyberVerse mini trainings and emphasizing their significance during open house or other departmental events. A combination of intentional advertising and word-of-mouth through users will be an effective way to recruit and retain students in these the niche CyberVerse areas.

6. Conclusion

In this paper, we focused on virtual reality technologies and how they can be implemented in improving cybersecurity education in higher learning institutions. These technologies are documented to enhance the learning ability for users by conveying complex concepts in a virtualized environment.

We focused on small colleges catering to less than 5000 students and outlined major challenges faced by them in using VR/AR technologies in teaching niche cybersecurity topic areas. We identified several such topic areas based on current curriculum frameworks and industry standards. We then proposed a four-fold method of incorporating this technology, together coined as CyberVerse, which included potential design and implementation ideas for teaching cybersecurity in small colleges. The techniques proposed in this paper are aimed at aiding these institutions to provide their students with exposure to the varied cybersecurity topics as well as give them an opportunity to leverage the limited resources for effective and improved cybersecurity teaching. Our future work plans to further investigate these techniques individually with case studies and user surveys.

Ethics Declaration: No ethical clearance was needed for the research described in this paper.

AI Declaration: I have used an AI tool to polish up figures 1 and 2 used in this paper. A part of the research example described in the paper had an AI generated component (BB84 simulator). No other uses of AI have been made in this paper.

References

Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information*, *11*(2), 121.

Childs, E., Mohammad, F., Stevens, L., Burbelo, H., Awoke, A., Rewkowski, N., & Manocha, D. (2023). An overview of enhancing distance learning through emerging augmented and virtual reality technologies. *IEEE transactions on visualization and computer graphics*, *30*(8), 4480-4496.

Cooper, G., & Thong, L. P. (2018). Implementing virtual reality in the classroom: Envisaging possibilities in STEM education. In *STEM education: An emerging field of inquiry* (pp. 61-73). Brill.

https://claude.ai/public/artifacts/bb2855d7-6584-47ab-b5dd-c34d727fd78e

https://github.com/smandal-metrostate/BB84-VR

https://qosf.org/project_list/

https://quantumflytrap.com/virtual-lab/

Ingalls, J. (2021). Viewpoint–Cybersecurity Data Visualization in the Next Dimension. *Ingalls Information Security, https://iinfosec. com/viewpoint*.

Kirschner, P. A. (2002). Cognitive load theory: Implications of cognitive load theory on the design of learning. *Learning and instruction*, *12*(1), 1-10.

Kullman, K., Ryan, M., & Trossbach, L. (2019). VR/MR supporting the future of defensive cyber operations. *IFAC-PapersOnLine*, *52*(19), 181-186.

Mandal, S. (2013). Brief introduction of virtual reality & its challenges. *International Journal of Scientific & Engineering Research*, *4*(4), 304-309.

Marr, B. (2019). *What is extended reality technology? A simple explanation for anyone. Forbes*.

Matsika, C., & Zhou, M. (2021). Factors affecting the adoption and use of AVR technology in higher and tertiary education. *Technology in Society*, *67*, 101694.

Neelakantan, S. (2019). Schools Face Barriers to VR Adoption in the classroom. *Tech, https://edtechmagazine. com/k12/article/2019/12/schools-face-barriersvr-adoption-classroom*.

Scholefield, S., & Shepherd, L. A. (2019, June). Gamification techniques for raising cyber security awareness. In *International conference on human-computer interaction* (pp. 191-203). Cham: Springer International Publishing.

Seo, J. H., Bruner, M., Payne, A., Gober, N., McMullen, D., & Chakravorty, D. K. (2019). Using virtual reality to enforce principles of cybersecurity. *The Journal of Computational Science Education*, *10*(1).

Skorenkyy, Y., Kozak, R., Zagorodna, N., Kramar, O., & Baran, I. (2021, March). Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education. In *Journal of Physics: Conference Series*(Vol. 1840, No. 1, p. 012026). IOP Publishing.

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. (2020, September). CyberVR: an interactive learning experience in virtual reality for cybersecurity related issues. In *Proceedings of the 2020 International Conference on Advanced Visual Interfaces* (pp. 1-8).

Wagner, P., & Alharthi, D. (2023). Leveraging vr/ar/mr/xr technologies to improve cybersecurity education, training, and operations. *Journal of Cybersecurity Education, Research and Practice*, *2024*(1), 7.

Zhu, Y., & Li, N. (2021). Virtual and augmented reality technologies for emergency management in the built environments: A state-of-the-art review. *Journal of safety science and resilience*, *2*(1), 1-10.