Immersive Learning: Understanding the Psychology of Crime Using Virtual Reality

Denise Ferebee, PhD.
Department of Math and Computer Science
Rust College
Holly Springs, MS, USA
0000-0003-4791-4638

Jerome Blakemore, PhD.
School of Social Work
Union University
Memphis, TN, USA
0009-0005-9590-6570

Marcus Kelly
Code Crew
Memphis, TN, USA
0009-0006-8919-4885

Zina Parker, EdD.
Division of Education
LeMoyne-Owen College
Memphis, TN, USA
0009-0004-3824-3646

Micheal Zhou
Division of Computer Science
LeMoyne-Owen College
Memphis, TN, USA

Tyana White
Division of Education
LeMoyne-Owen College
Memphis, TN, USA

Farheen Dahani
Division of Computer Science
LeMoyne-Owen College
Memphis, TN, USA

Jiya Webster
Division of Education
LeMoyne-Owen College
Memphis, TN, USA

***Abstract*—Teaching cybersecurity professionals has changed from applying puzzle-based learning scenarios [1], general tabletops [2], and general gamification [3] to an immersive learning environment [4]–[7]. In today's teaching environment, there are known methods to teach cybersecurity tool techniques. However, beyond the technical aspect, cybersecurity professionals need to understand the psychology of crime. These teaching and learning needs have become more prevalent in criminal justice, education, and computer science degree programs and aspects of job professions because learners need to understand and be able to recognize why crimes are committed. Thus, opening another major area of research in cybersecurity [8].**

Teaching someone what it means to protect systems, networks, and programs from digital attacks is difficult. Each person needs some frame of reference. Through their personal frame of reference, they discern and consume the information and find a basis for its purpose. This is known as the learning process and each individual journey is different. The learning process is affected by personal experience. Thus, creating a climate for misunderstanding through applying personal experiences to a situation that may have had a different personal or professional interaction. Because of misunderstandings and unconscious bias that occur in this type of learning structure, the misunderstandings and unconscious bias have the potentiality of being propagated into professional career interactions and investigations. Thus, this project will present a learning platform/framework to explore cybersecurity methods, discern interactions, explore the psychology of why a crime is committed through a collaborative virtual reality (VR) immersive environment.

Keywords—cybersecurity, education, learning tools, psychology of crime, implicit bias

This work was supported by the NCAE-C Cyber Curriculum and Research 2020 Program: NCAE-C-003-2020: [Grant No. H98230-20-1-0406].

I. INTRODUCTION

Cybersecurity education has been a societal focus because of the advances in technology and the threats that they pose. Getting learners prepared for cybersecurity jobs is an extensive learning process. Students are presented information by various methods. The hardest thing to teach a student is how to observe personal interactions and how to glean information. Understanding personal interactions is very important in cybercrime investigation because it helps to establish a motivation for the crime. There is a more systematic approach to teaching technical analysis in field aspects such as digital forensics, network forensics, etc. These methods include the process of collecting, processing, preserving, analyzing, and presenting computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations. Teaching concepts about social interactions in cybercrime is complex because they involve complex situational analysis and understanding. Every cybercrime is different, there is no standard format for analyzing. Thus, requiring learners to be active participants in a situated learning environment where crime scene interactions can be recreated and discussed. We believe this method will enhance the learner's perspective and allow them to establish an understanding of motivational factors. Cybersecurity exercises require an activity approach through which learners explore and analyze a situation requiring the use of forensic tools, criminal activity motivation analysis, and risk mitigation. This approach should be collaborative and adaptable to maximize its effectiveness. Therefore, our approach is to provide a collaborative, immersive, VR learning environment based on the need to explore the psychology of crime, unconscious bias, and provide students with a frame of reference to make appropriate decisions based on evidence. The sections of this document will consist of the following: related work, proposed event correlation, proposed methodology, implementation, and future work.

II. LITERATURE REVIEW

A. *Implicit Bias*

When teaching cybersecurity, the hardest thing to convey to a student is recognizing bias and how it can affect how a crime is investigated. People are products of their experiences, and those experiences affect decision making and perception. Currently, people have been using virtual reality (VR) for diversity training [9], [10]. However, there has not been much research done in classroom application for cybersecurity crime scene analysis.

B. *Psychology of Crime*

The major portion of crime scene analysis is understanding the motivation for the crime. The need for understanding the psychology of crime is becoming a major factor in crime prevention (i.e., understanding the motivation in order to mitigate the risk) [8], [11], [12].

C. *Pedagogical Methods of Teaching*

Many of the current methods for teaching about cybersecurity have been using gamification [13]. Other Pedagogical methods include exercises and tabletop scenarios both on paper and electronic [2], [14], [15]. However, these methods do not tackle the aspect of implicit bias.

III. METHODOLOGY

The overall goal of the proposed project is to create a collaborative, immersive, virtual reality learning environment (CI-VR-LE) in order to introduce and examine how learners determine perspectives about interactions between people that commit crimes and why they commit crimes. There are many pedagogical aspects in teaching cybersecurity [1], [14], [15]. However, this project will cover immersive learning and experiential learning in a virtual environment.

This technical objectives will include the following: (1) Create CI-VR-LE tabletops to provide learners with a virtual, collaborative, playable cybercrime scene; (2) study the interactions between virtual players; (3) provide students with a virtual environment to study the psychological aspects of cybercrime; (4) study the effectiveness of the simulation with providing learners aspects of criminology that they have not been exposed to from an interdisciplinary perspective; and (5) develop cybercrime scenarios to be used in cybersecurity courses in the education, criminal justice, and computer science departments. Thus, providing a platform where learners can study interactions (i.e., the people committing cybercrime and theirs) to learn about unconscious/unintentional bias.

To conduct the research associated with CI-VR-LE, several steps/tasks/activities will need to be completed. These consist of reviewing current pedagogy methods that deal with experiential learning, immersive learning, and gamification; focusing on the psychology of crime; examining how cybercrime is approached in the criminal justice field; establishing what is considered as red flags about unintentional or unconscious bias; review current pedagogical approaches to cybersecurity; and establish how virtual reality can be used to simulate lessons on human interactions. Various techniques from the fore mentioned subject areas will be combined to create a CI-VR-LE. Therefore, this section will provide an explanation of the technical approach and the tasks associated in the proposed research as shown in Fig. 1. These processes/tasks are explained as follows:

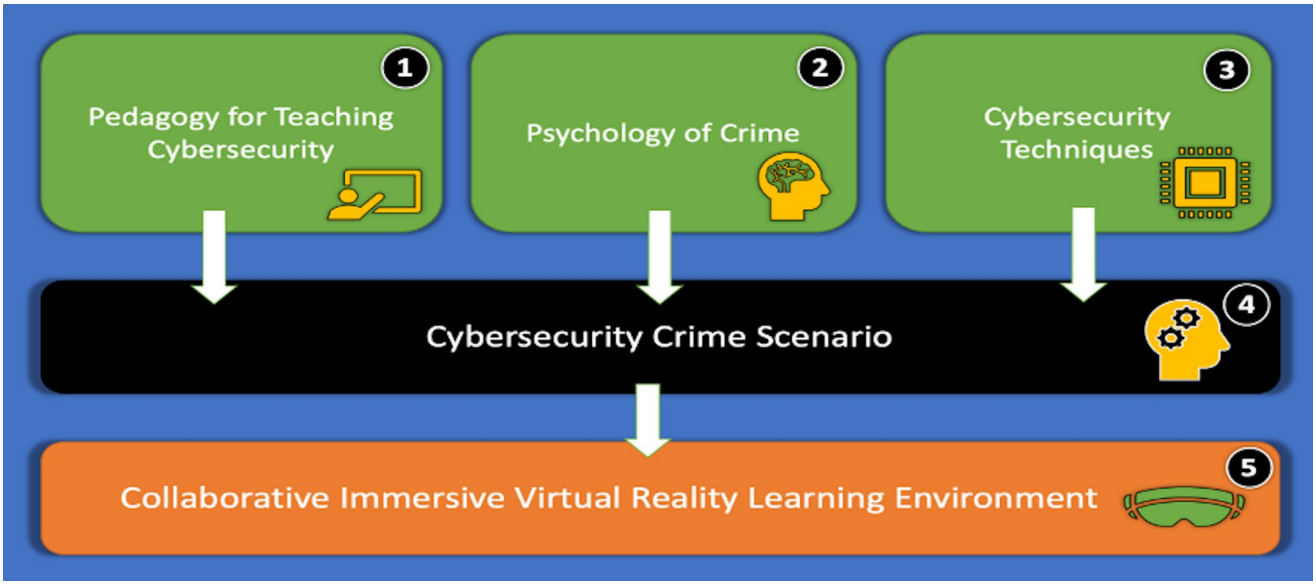

Fig. 1. Collaborative Immersive Virtual Reality Learning Environment

Process 1:

Pedagogy for Teaching Cybersecurity – This process consists of reviewing the aspects of immersive and experiential learning, applying case studies, game-based learning, the exploration of learning outcomes, and the creation of rubrics to cybersecurity course development and activity creation [1]–[5], [14]–[23]. Once the base pedagogy has been established, it must be applied to the cybersecurity scenario creation in order to establish the appropriate outcomes that meet the A (audience), B (behavior), C (conditions), and D (degree) characteristics of outcome creation for the CI-VR-LE [24]. These outcomes will be used to evaluate learner mastery of concepts covered in the activities created during this project. Then, they will be incorporated into education, computer science, and criminal justice courses during the course design process. Specifically, in education, they will be used to teach teachers how to create cybersecurity courses at the K-12 and post-secondary levels.

Process 2:

Psychology of Crime – Through this process the foundation of criminal psychology will be incorporated into the cybersecurity curriculums for education, criminal justice, and computer science [8], [25]. Next, cybercrime scenarios will be developed that focus on interactions between the people committing crimes [11], [12]. The scenarios will be evaluated by the researchers in education, criminal justice, and computer science to determine if they portray a realistic view of what happens during the act of committing the crime.

Process 3:

Cybersecurity Techniques – In this process cybersecurity scenarios will be designed based on current cybercrimes [1], [2], [26], [27]. These scenarios will be reviewed by the education, criminal justice, social work, and psychology specialists. Next, they will be broken down into perceived interactions. Once these interactions have been documented, it will be determined as to which cybersecurity technique (i.e., network security, host security, digital forensics, etc.) will be incorporated. Thus, teaching the interactions will be incorporated with teaching skills for a holistic approach to teaching cybersecurity principles.

Process 4:

Cybersecurity Crime Scenario – All of the components will be incorporated from Processes 1-3 to create the CI-VR-LE scenarios. These scenarios will be storyboarded to have a clear flow between scenes and to verify that the character interactions are captured. Researchers will use VR development products such as Oculus Quest, Unity, Blender, and Maya to translate the storyboard scenes into a playable crime scene scenario [28]–[31]. Each learner will have the ability to collect clue items that provide information in reference to solving the cybercrime. The type of clue item will co-inside with a specific cybersecurity technique/skill the learner needs to demonstrate. Each scenario will be tested, evaluated, and modified based on flaws that appear. Also, each scenario will be incorporated into a set of playable scenario type set that will be organized based on categories.

Process 5:

CI-VR-LE Creation – All of the scenarios that will be used in the education, criminal justice, and computer science courses will be incorporated into a multi-player environment. This will allow learners to collaboratively interact with the simulated environment and discuss the interactions in real time. This will allow the instructor to discuss their perceptions of the crimes and the crime scene characters. Thus, providing an academic environment to study the psychology of crime in an immersive environment that will provide more information than just reading a scenario and guessing about the interactions. Also, it will allow students to express how they view the scenario via their own experiences which will allow the instructor to make corrections for unconscious bias.

IV. IMPLEMENTATION

The project consists of seven major components as shown in Fig. 2 where together they will produce an immersive VR environment.

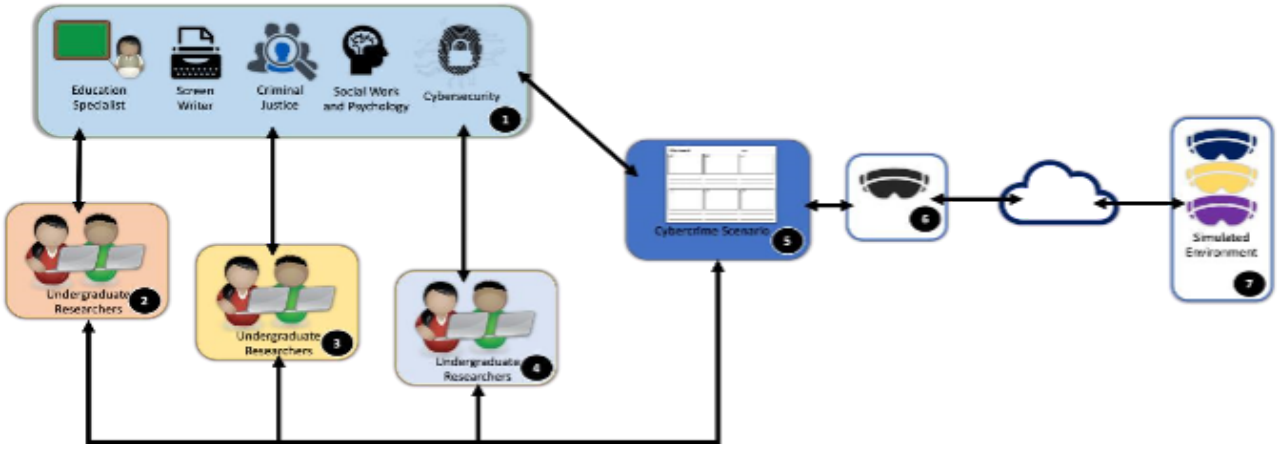

Fig. 2. CI-VR-LE Components

These components and processes are as follows:

Component 1:

CI-VR-LE Cybercrime Scenario Creation Team will collaborate to create types of cybercrimes scenarios that will be relevant in courses taught in education, criminal justice, and computer science courses. The education specialist will determine the pedagogical techniques used in order to improve teaching effectiveness [1], [4], [14]–[18]. The criminal justice specialist will provide psychological aspects of cybercrimes that focus on interactions between criminals and how this is currently being taught to criminal justice professionals and potential legal aspects [2], [32]. The social work and psychology specialist will provide the aspects of how cybercrime affects communities and the potential backgrounds that can lead people to become at risk [8]. The cybersecurity specialist will provide the cybersecurity expertise for teaching about cybercrimes, the tools used, and the technology creation aspects that will be needed to create the CI-VR-LE. Each specialty area will work with undergraduate researchers to incorporate cybersecurity fundamentals, teaching aspects, and research into the corresponding programs via studying the psychology of crime, unconscious bias, and collaborative work environments.

Component 2:

Undergraduate Education Researchers will work with the education specialist on how to implement goals into each cybercrime scene scenario. An example of these general goals and objectives are as follows and will be modified based on how the scenarios are structured per course activity:

- Students will improve and demonstrate his/her logical thinking skills.
    - Students will make responsible decisions in ___ out of ___situations.
    - Students will solve problems in ___ out of ___situations.
    - Students will correct inferences in ___ out of ___situations.
- Students will improve and demonstrate his/her critical thinking skills.
    - Students will demonstrate comprehension of multiple meaning words in ___ out of ___ trials.
    - Students will demonstrate generalization of knowledge by placing new knowledge by placing new knowledge into several different categories with ____% accuracy.
    - Students will generalize information learned to quizzes, test, etc. in ___out of ___ trails with ___% accuracy.
- Students will perform academically at the required ability level.
    - Students will perform academic tasks with ___% accuracy.
    - Students will meet a ___% level of mastery on academic tasks.
    - Students will perform academic tasks on the required ability level on ___ out of ___ trails.
    - Students will perform tasks designed to meet the required level ability with ___% accuracy.
- Students will follow written directions.
    - Students will read all directions before beginning tasks and activities on __ out of __trials.
    - Students will follow one-step, two-step, multi-step directions on ___ out of ___ trials.
    - Students will ask for clarification of written directions not understood on ___ out of ___ trails.
- Students will follow multi-step directions
    - Students will follow one-step, two-step, multi-step verbal directions on ___ out of ___trails.
    - Students will follow verbal directions in correct sequential order on ___ out of ___ trails.
    - Students will demonstrate the ability to follow verbal directions by listening carefully and completing the task with ___% accuracy on ___ out of ___ trails.

Component 3:

Undergraduate Criminal Justice Researchers will work with the criminal justice and social work and psychology specialists to determine the types of behaviors and interactions that should be recognized in cybercrime and what may be the reasons why the criminal may exhibit these behaviors. These behaviors will be incorporated into each cybercrime scene scenario to simulate the interactions for learners. The goals of their work result in being able to provide:

- Learners can pursue internships with criminal justice agencies in the area (i.e., locally).
- Tools created via this effort can be used by community partners to perform inhouse training for current and future employees in cybersecurity.
- Provide law enforcement agencies with skilled workers (i.e., after graduation) that are equipped to enhance their cybersecurity programs.
- Increase the capacity of students and allied criminal justice agencies in cybersecurity.
- Foundation for studying the legal aspects with managing technology in criminal justice.

Component 4:

Undergraduate Computer Science Researchers will work with the cybersecurity specialist to use virtual reality (VR) technology to create the immersive cybercrime scenarios based on the storyboards created. Additional cybersecurity activities will be created to supplement the scenarios in order to capture tool use.

Component 5:

CI-VR-LE Cybercrime Scenario Storyboards will be created by a screen writing specialist based on the aspects designed through the education, criminal justice, social work and psychology, and cybersecurity/computer science specialists' efforts. These will be evaluated to make sure that the behaviors are being captured/recognized.

Component 6:

The virtual reality translation of CI-VR-LE cybercrime scenario storyboards is where the multi-user environment is created. Undergraduate computer science researchers will use VR equipment and software to complete this effort. The team will evaluate the demos for fine tuning and determine if the cybercrime concepts are clear.

Component 7:

Multi-user CI-VR-LE simulated environment is the prototype environment that will be used in the classroom. Learners will use VR equipment in activities to share an experience and gather information about the cybercrime or situation being presented. The learners will discuss the scenario in class to understand behaviors of the computer-generated participants (i.e., avatars) and theirs. This will provide the platform to discuss the concepts of criminal psychology in a non-threatening environment.

V. RESULTS

After the software was created, testing with students began to get a view of which a written description as opposed to a virtual reality/immersive experience provided better understanding of interactions. Thus, a process was used for developing the qualitative data analysis included individual responses to two forms of review, including paper narrative and immersive techniques.

Transcripts were generated verbatim from the online responses provided by each research participant. Each research team member independently organized the data to ensure that the early findings were not developed out of group think bias. This process helped to ensure reliability and validity in the analysis process.

Findings were then organized into a set of ideas, concepts, and overarching themes in the data. The research team then reviewed these to ensure a high level of confidence that the findings reflected the respondents' perspective and not the potential bias of research team members.

A systematic and consistent approach was used for data collection. The entire team participated in the session, where participants reviewed the two cases. The initial review of the cases focused on narratives presented in paper format. The second review used exclusively immersive methods for the review. Each participant completed a questionnaire to provide their perspective regarding the two cases. A focus group (i.e., exit interview) was held after the completion of round two to assess participant perspectives on which method had more utility. The team did not start off with a set of assumptions or a working hypothesis, so the findings do not represent any surprises.

The researchers independently assessed the data to ensure external validation, and the research group compared findings. There appeared to be good integrated reliability. In the process of collective review, there were no inconsistent or conflicting findings.

The data analysis aimed to identify significant themes and provide interpretations of ideas in the current context. The focus group was modified and conducted using an exit interview summary process where each participant provided their perspective on the differences between the paper narrative and the 3D virtual immersive content. Twelve (12) students participated in the exit interview. Participants were HBCU college students ranging in age from 19 to 24. Their primary area of study was computer science and cybersecurity.

Students indicated that virtual reality was the method of preference, although many indicated that combining them reached the end goal. Only two were neutral, and one indicated that the paper narrative was the option of choice.

VI. FUTURE WORKS

We will continue this research by looking at other ways to enhance incorporating the psychology of crime into current cybersecurity curriculum and pedagogical approaches for teaching about implicit bias.

ACKNOWLEDGEMENT

This paper and the research behind it would have not been possible without our screenwriter Princeton James and Princeton James Productions. The effort and patience used to capture the scenarios used in this research made the work more realistic and meaningful.

REFERENCES

[1] D. Dasgupta, D. M. Ferebee, and Z. Michalewicz, "Applying Puzzle-based Learning to cyber-security education," *Proceedings of the 2013 Information Security Curriculum Development Conference, InfoSec CD 2013*, pp. 20–26, 2013, doi: 10.1145/2528908.2528910.

[2] D. Ferebee, C. Butler, D. Dasgupta, and M. Kelly, "Digital forensics the open way: A tabletop approach to common scenarios," in *The Open Organization Guide for Educators*, 2019, pp. 198–211.

[3] G. Jin, M. Tu, T.-H. Kim, J. Heffron, and J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students," *Journal of Education and Learning (EduLearn)*, vol. 12, no. 1, pp. 150–158, Feb. 2018, doi: 10.11591/edulearn.v12i1.7736.

[4] S. Tan, "The rise of immersive learning," *Journal of Applied Learning and Teaching*, vol. 2, no. 2, pp. 91–94, Dec. 2019, doi: 10.37074/jalt.2019.2.2.12.

[5] D. Russell, "The Design of Immersive Virtual Learning Environments Utilizing Problem-Based Learning Templates," 2015, pp. 105–123. doi: 10.4018/978-1-4666-9629-7.ch005.

[6] J. Parong and R. E. Mayer, "Learning science in immersive virtual reality.," *J Educ Psychol*, vol. 110, no. 6, pp. 785–797, 2018, doi: 10.1037/edu0000241.

[7] R. L. Jackson and E. Fagan, "Collaboration and learning within immersive virtual reality," *Proceedings of the third international conference on Collaborative virtual environments* - CVE '00, 2000, doi: 10.1145/351006.351018.

[8] J. Taylor-Jackson, J. McAlaney, J. L. Foster, A. Bello, A. Maurushat, and J. Dale, "Incorporating Psychology into Cyber Security Education: A Pedagogical Approach," *Financial Cryptography and Data Security*, pp. 207–217, 2020, doi: 10.1007/978-3-030-54455-3_15.

[9] "How Virtual Reality Is Used To Help Recognize Unconscious Biases : NPR." https://www.npr.org/2021/05/19/998137110/how-virtual-reality-is-used-to-help-recognize-unconscious-biases (accessed Sep. 16, 2023).

[10] "How Police Departments Use VR for Implicit Bias Training." https://www.apexofficer.com/resources/how-police-departments-use-vr-for-implicit-bias-training (accessed Sep. 16, 2023).

[11] G. Kirwan and A. Power, *Cybercrime: The psychology of online offenders*. Cambridge University Press, 2013.

[12] G. Kirwan and A. Power, "The psychology of cyber crime : concepts and principles," p. 277, 2012.

[13] [C. J. Cornel, D. C. Rowe, and C. M. Cornel, "Starships and cybersecurity: Teaching security concepts through immersive gaming experiences," in SIGITE 2017 - *Proceedings of the 18th Annual Conference on Information Technology Education*, Association for Computing Machinery, Inc, Sep. 2017, pp. 27–32. doi: 10.1145/3125659.3125696.

[14] M. Karjalainen, T. Kokkonen, and S. Puuska, "Pedagogical Aspects of Cyber Security Exercises," in *Proceedings - 4th IEEE European Symposium on Security and Privacy Workshops, EUROS and PW 2019*, Institute of Electrical and Electronics Engineers Inc., Jun. 2019, pp. 103–108. doi: 10.1109/EuroSPW.2019.00018.

[15] A. Arabo and M. Serpell, "Pedagogical Approach to Effective Cybersecurity Teaching," *Transactions on Edutainment XV*, pp. 129–140, 2019, doi: 10.1007/978-3-662-59351-6_11.

[16] D. Tang, C. Pham, K. Chinen, and R. Beuran, "Interactive cybersecurity defense training inspired by web-based learning theory," *2017 IEEE 9th International Conference on Engineering Education (ICEED)*, 2017, doi: 10.1109/iceed.2017.8251171.

[17] M. Slater, "Implicit Learning Through Embodiment in Immersive Virtual Reality," *Smart Computing and Intelligence*, pp. 19–33, 2017, doi: 10.1007/978-981-10-5490-7_2.

[18] A. Klippel, J. Zhao, D. Oprean, J. O. Wallgrun, and J. S. K. Chang, "Research framework for immersive virtual field trips," in *26th IEEE Conference on Virtual Reality and 3D User Interfaces*, VR 2019 - Proceedings, Institute of Electrical and Electronics Engineers Inc., Mar. 2019, pp. 1612–1617. doi: 10.1109/VR.2019.8798153.

[19] Y. Cai, "Using Case Studies To Teach Cybersecurity Courses," 2018. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/ Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/3

[20] M. Memon, "Experiential Learning versus Immersive Learning - Training Industry", Accessed: Sep. 16, 2023. [Online]. Available: https://trainingindustry.com/articles/content-development/experiential-learning-versus-immersive-learning/

[21] A. Y. Kolb and D. A. Kolb, "Experiential Learning Theory as a Guide for Experiential Educators in Higher Education," 2017. [Online]. Available: https://nsuworks.nova.edu/elthe/vol1/iss1/7/

[22] M. K. Thomas, A. Shyjka, S. Kumm, and R. Gjomemo, "Educational Design Research for the Development of a Collectible Card Game for Cybersecurity Learning," *J Form Des Learn*, vol. 3, no. 1, pp. 27–38, Jun. 2019, doi: 10.1007/s41686-019-00027-0.

[23] J. K. Mcdonald *et al., Designing Authentic Cybersecurity Learning Experiences: Lessons from the Cybermatics Playable Case Study*. [Online]. Available: https://hdl.handle.net/10125/59689

[24] "Writing Learning Outcomes - Information Literacy Toolkit: Resource for Teaching Faculty - Research Guides at University of Maryland Libraries." Accessed: Jan. 19, 2024. [Online]. Available: https://lib.guides.umd.edu/InfoLitToolkit/learningoutcomes/writing

[25] D. T. Morse, "Learning Styles: Psychology Shouldn't Condone Mythology," 2011. [Online]. Available: www.symbiosisonline.org; www.symbiosisonlinepublishing.com

[26] N. Falkner, R. Sooriamurthi, and Z. Michalewicz, "Puzzle-Based Learning for Engineering and Computer Science," 2010.

[27] M. E. Whitman and H. J. Mattord, *Principles of Information Security*. Cengage Learning Asia Pte Limited, 2018. [Online]. Available: https://books.google.com/books?id=NEjQxgEACAAJ

[28] "Meta Quest 2: Immersive All-In-One VR Headset | Meta Store | Meta Store." https://www.meta.com/quest/products/quest-2/ (accessed Sep. 16, 2023).

[29] "Unity Real-Time Development Platform | 3D, 2D, VR & AR Engine." https://unity.com/ (accessed Sep. 16, 2023).

[30] "Maya Software | Get Prices & Buy Official Maya 2024 | Autodesk." https://www.autodesk.com/products/maya/overview?term=1-YEAR&tab=subscription&plc=MAYA (accessed Sep. 16, 2023).

[31] "blender.org - Home of the Blender project - Free and Open 3D Creation Software." https://www.blender.org/ (accessed Sep. 16, 2023).

[32] A. Rege, E. Parker, and T. McJunkin, "Using a critical infrastructure game to provide realistic observation of the human in the loop by criminal justice students," in *Proceedings - 2017 Resilience Week, RWS 2017*, Institute of Electrical and Electronics Engineers Inc., Oct. 2017, pp. 154–160. doi: 10.1109/RWEEK.2017.8088665.