Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 7

October 2023

Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations

Paul Wagner
University of Arizona, paulewagner@arizona.edu

Dalal Alharthi
University of Arizona, dalharthi@arizona.edu

Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations

Abstract

The United States faces persistent threats conducting malicious cyber campaigns that threaten critical infrastructure, companies and their intellectual property, and the privacy of its citizens. Additionally, there are millions of unfilled cybersecurity positions, and the cybersecurity skills gap continues to widen. Most companies believe that this problem has not improved and nearly 44% believe it has gotten worse over the past 10 years. Threat actors are continuing to evolve their tactics, techniques, and procedures for conducting attacks on public and private targets. Education institutions and companies must adopt emerging technologies to develop security professionals and to increase cybersecurity awareness holistically. Leveraging Virtual/ Augmented/Mixed/Extended Reality technologies for education, training, and awareness can augment traditional learning methodologies and improve the nation's cybersecurity posture. This paper reviews previous research to identify how distance and remote education are conducted generally, and how Virtual/Augmented/Extended/Mixed reality technologies are used to conduct cybersecurity awareness training, cybersecurity training, and conduct operations. Finally, barriers to adopting these technologies will be discussed. Understanding how these technologies can be developed and implemented provides one potential way of overcoming the cybersecurity workforce gap and increasing the competencies and capabilities of cybersecurity professionals.

Keywords

Virtual Reality, Augmented Reality, Extended Reality, Cybersecurity Training and Education, Security Awareness Training

Leveraging VR/AR/MR/XR Technologies to Improve Cybersecurity Education, Training, and Operations

Paul Wagner
Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona
paulewagner@arizona.edu
https://orcid.org/0000-0001-5914-0479

Dalal Alharthi
Cyber, Intelligence, and Information Operations
University of Arizona
Tucson, Arizona
dalharthi@arizona.edu
https://orcid.org/0000-0003-0299-024X

***Abstract*— The United States faces persistent threats conducting malicious cyber campaigns that threaten critical infrastructure, companies and their intellectual property, and the privacy of its citizens. Additionally, there are millions of unfilled cybersecurity positions, and the cybersecurity skills gap continues to widen. Most companies believe that this problem has not improved and nearly 44% believe it has gotten worse over the past 10 years. Threat actors are continuing to evolve their tactics, techniques, and procedures for conducting attacks on public and private targets. Education institutions and companies must adopt emerging technologies to develop security professionals and to increase cybersecurity awareness holistically. Leveraging Virtual/ Augmented/Mixed/Extended Reality technologies for education, training, and awareness can augment traditional learning methodologies and improve the nation's cybersecurity posture. This paper reviews previous research to identify how distance and remote education are conducted generally, and how Virtual/Augmented/Extended/Mixed reality technologies are used to conduct cybersecurity awareness training, cybersecurity training, and conduct operations. Finally, barriers to adopting these technologies will be discussed. Understanding how these technologies can be developed and implemented provides one potential way of overcoming the cybersecurity workforce gap and increasing the competencies and capabilities of cybersecurity professionals.**

Keywords—Virtual Reality, Augmented Reality, Extended Reality, Security Awareness Training, Cybersecurity Training and Education

I. Introduction

The United States faces persistent and consistent threats from a variety of threat actors which threaten the American way of life. Combatting these actions requires a strong workforce that is properly trained to combat current and emerging threats. Unfortunately, as of 2021, there are over 3 million unfilled cybersecurity jobs with less than half of that number of workers currently in the field [1]. Most companies believe that this problem has not improved and nearly 44% believe it has gotten worse over the past 10 years [2]. This paper aims to shed light on this complex challenge by exploring how individuals become cybersecurity professionals. Current paths to cybersecurity expertise include formal education at universities or technical institutions, professional certifications, online learning platforms, books, or boot camps. Additionally, hands-on experience can be obtained through internships, apprenticeships, or on-the-job training. The cybersecurity skills gap continues to widen despite the plethora of free and fee-based education and training opportunities. This problem is further exacerbated by the continuously evolving threat landscape and the requirement to continuously train and hone knowledge, skills, and abilities. This paper proposes that leveraging Virtual / Augmented / Extended / Mixed Reality (*R) technologies can improve the overall cybersecurity posture by providing security awareness, education, and technical training, and support security operations. To guide our research, we will explore how distance/remote cybersecurity education works, the potential of *R technologies to improve training and operations, and the main barriers to their adoption.

This work will result in a comprehensive taxonomy of collected resources, applications, and experiences to enhance cybersecurity awareness, training, and operations. Best practices and constraints will be outlined to enable educators, executives, and employees to integrate *R technologies in these areas. Finally, gaps in research, technology, and content will be identified to facilitate future research.

II. Proposed Work

A. Research Design and Methodology

The author used a systematic literature review (SLR) technique to find relevant academic articles from 2010 to 2021. Relevant information was extracted from select articles to inform analysis and discussion. The steps involved in the SLR process include:

1) Define the research questions.
2) Determine the data sources and search process.
3) Inclusion and Exclusion Criteria.
4) Results of searching and data extraction.
5) Analysis and Discussion.

B. Research Questions

1) How is distance/remote education conducted generally; for cybersecurity awareness training, technical training, and cybersecurity operations?

2) Can *R technologies improve or enhance cybersecurity training and operations?

3) If *R technologies are determined to be effective in improving or enhancing cybersecurity training and operations, what are the barriers to widespread adoption?

C. Data Sources and Search Process

A variety of sources were used to identify sources for this research including Google Scholar, IEEE, Elsevier, EBSCO, Proquest, and other library resources. Additionally, current industry trend reports were analyzed to identify current and relevant statistics to support research objectives. Search terms included but were not limited to Virtual Reality, Augmented Reality, Mixed Reality, Extended Reality, Cybersecurity Awareness Training, Security Awareness Training, Cybersecurity Technical Training, and Cybersecurity Operations. The search limited results from 2010 to the present. This range was necessary to accurately identify the evolution of online education, remote learning, and *R technologies.

D. Inclusion and Exclusion Criteria

Given the limited, specific research on the application of *R technologies for cybersecurity, the author applied a liberal inclusive set of search criteria. Full-text journal articles were used to identify and analyze the use of *R technologies in education and online learning. Information from these articles was extrapolated for their potential use for the specific use cases of cybersecurity awareness, training, and operations. Editorials, trade journals, and other online resources were used to identify the latest statistics and applications of *R technologies for these purposes.

Search Results

Search results can be broadly categorized into four categories of education, training, awareness, and adoption. Some results span education and training or awareness and training. The resulting table (Appendix 1) provides the authors, year, title, associated category(s), main findings, limitations if applicable, any additional information that can aid future researchers in identifying relevant information. For the purposes of this paper education, training, awareness, and adoption are defined as follows:

1) Education – Goes beyond training and awareness and typically aligned with formal education institutions like colleges or universities. Integrates all security skills and competencies from various functional specialties into a common body of knowledge [34].

2) Training – attempts to produce relevant and needed skills and competencies for a specific topic [34].

3) Awareness – focus attention on a particular topic which are intended to allow individuals to recognize and react appropriately to the topic [34].

4) Adoption – refers to the the technology being integrated into education, training, and operational settings.

III. 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 [3]. This equipment and technology provide users with different experiences classified as follows and depicted in Figure 1:

1) Virtual Reality (VR) – Users are completely immersed in a computer-generated reality.

2) 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.

3) Mixed Reality (MR) – moves beyond augmented reality allowing users to interact with virtual objects that are placed in the real world.

4) Extended Reality (XR) – an umbrella term for all immersive technologies currently available and still to be created [4].

Figure 1 – Milgram's MR Continuum [5]

For the purposes of this paper, the designation "*R" will be used to encompass all virtual reality technologies as defined in the previous section. 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. *R technologies incorporate software and hardware components to support human-computer interactions. The software's role is to build an interactive environment for users. The software must be capable of 3D modeling, a *R engine, and a physics engine capable of building the environment [15]. Hardware provides a type of middleware to input data and real-world information. Additionally, hardware injects and receives feedback and information into/from the virtual environment. *R enhances the user's learning ability, conveniently conveys complex concepts, and demonstrates those concepts from a virtualization perspective. Additionally, *R provides bidirectional communication between users and computers. This allows researchers and instructors with rich information on how users stimulate the virtual environment and the impact the virtual environment has on users.

Traditionally, users interacted with virtual reality through controllers that imitated a pointer or hand gestures at a rudimentary level. Advances in technology allow users to immerse themselves and interact with virtual environments in new ways. This includes eye-tracking, optical body tracking, gloves, optical hand gestures, muscular/spatial, neural interfaces, and various haptic and sensory feedback devices [6]. Throughout the remainder of this paper VR/AR/MR/XR technologies will be referred to as *R.

IV. Related Work

Research on remote education in emergencies has focused on humanitarian crises, natural disasters, and armed conflict and has existed for decades [7]. COVID-19 caused worldwide disruption of traditional learning modalities forcing educational institutions to evaluate effective modalities for remote education. This transition to online learning was hindered by a lack of planning, design, and development of content for

effective transmission of information to remote students. Based on this, it is important to properly plan when integrating *R, emerging technologies, and simulations for education and training purposes.

*A. *R for General Education*

Online learning has followed asynchronous, synchronous, and flipped classroom models. Asynchronous models provide flexibility allowing students to interact with content at their own pace. Synchronous models mimic traditional face-to-face classes. Technology has facilitated a more interactive and engaging experience for students through the use of collaboration platforms, learning management systems, screen-sharing, and "virtual black/whiteboards." Flipped classroom models provide lectures and content for students to review at home and utilize classroom time for more interactive and engaging activities.

Distance learning presents a variety of challenges including social interaction, student engagement and focus, and comprehension and information retention [5]. Research addressing social interaction concerns has led to positive improvements in leveraging *R technologies. *R has been used to create collaborative spaces, integrated conferencing to increase the sense of presence and integrate user movement and visual cues, and overlay drawings and graphics to enhance video calls [5]. Further, comparative research on social interactions in virtual and realworld environments determined that *R experiences were equally effective at allowing participants to engage and communicate socially [5].

Engaging students has been a problem for traditional and online learning. Technology, social media, and other distractions interfere with a variety of educational modalities. This can be especially true for asynchronous learning since students do not have access to non-verbal cues associated with face-to-face learning. Additionally, technology and connectivity issues can decrease the feeling of connectedness and engagement with the material. Studies using augmented reality books and augmented reality applications have shown increases in student motivation and engagement. Virtual reality allows users to move around the virtual environment and interact with objects to create a sense of immersion. Immersive environments blend a digital computer-generated environment with the real world. Additionally, external distractions are minimized or removed using *R technologies.

*R technologies have demonstrated their ability to improve knowledge acquisition and understanding, concept retention, and improving understanding of abstract and complex topics [5]. Additionally, studies have shown that *R has increased motivation and attitudes towards learning which has been positively correlated with students' ability to comprehend and retain information.

*B. *R For Cybersecurity Awareness Training*

Conducting cybersecurity awareness training is one of the most cost-effective and beneficial methods to reduce cybersecurity breaches and incidents. Cybersecurity awareness can be described as, "The harmonization of capabilities in people, processes, and technologies: to secure and control both authorized and/or unlawful access, disruption, or destruction of electronic computing systems (Hardware, software, and networks), the data and information they hold [18]." It is estimated that 95% of cybersecurity breaches are caused by human error demonstrating the need for improved security awareness training [8]. Despite these facts, traditional cybersecurity awareness training programs have proven ineffective and fail to reduce organizational risk. This is due to several reasons.

Cybersecurity awareness is essential for worldwide internet users of all ages addressing both domestic and workplace environments and risks as applicable. Training the younger population comes with its own set of challenges. First, accepting and understanding security concepts is exacerbated by taking a one-size fits all approach to security awareness messaging and content. Additionally, younger populations are typically not risk-averse and tend to overshare information. This behavior introduces data privacy issues.

Also, many (55%) organizations do not offer mandatory security awareness training, and organizations that do require it do so sparingly [9]. Additionally, some companies that do provide training do so to meet compliance requirements which result in a "check the box" mentality instead of instilling a security-minded culture. This leads to a lack of employee buy-in. Further, much of the content is not engaging and may involve a slideshow, video, or other materials that require little or no interaction. Finally, organizations don't have a holistic and realistic training plan that constantly evaluates the overall security posture for the organization and employees' part in that. Research by He and Zhang [17] identified similar issues outlined below:

- Employee boredom and completing requirements quickly without paying attention to the material
- Employee lack of interest and motivation due to lack of incentives
- Training not tailored to employee roles, learning styles, or needs
- Training content is not relevant or updated and maintaining relevance is not cost-effective for organizations

*C. *R For Cybersecurity Technical Training*

Over 3 million unfilled cybersecurity jobs demonstrate a critical shortage for organizations creating a national security risk [10]. Additionally, cybersecurity professionals must maintain their skills and develop new skills to remain relevant and keep pace with threat actors. Despite this, nearly 82% of respondents from an Information Systems Security Association (ISSA) survey stated general job requirements prohibit them from sustaining their knowledge and skills [11]. Leveraging *R technologies may be one method of overcoming this training deficit. Various studies have demonstrated that training provided through *R technologies resulted in higher enjoyment by users and increased changes in behavior [12]. Additionally, immersive learning involving authentic inquiry, active observation, peer coaching, and reciprocal teaching provides

optimal learning [13]. Research on this determined a 75% higher retention of information and increased potential for making fewer mistakes after *R training. It is important to note that this research determined that *R training should complement other training to provide comprehensive training and experiences across a variety of problem sets.

*D. *R For Cybersecurity Operations*

Cybersecurity operations is a very broad field including incident response, penetration testing, digital forensics, cyber threat intelligence, cyber defense, and offensive operations conducted by authorized government entities. Specifically, the National Institute of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE) Framework outlines seven domains and 33 specialized areas for cybersecurity jobs. *R technologies provide multiple methods to develop content, training, and tools to conduct daily operations across these domains.

For example, *R technologies provide Security Operations Center (SOC) analysts the ability to conduct operations anywhere while still having access to the infrastructure, services, tools, alerts, and controls provided by the fixed physical infrastructure. Additionally, *R can layer visual cues on alerts to assist Tier-1 SOC analysts conduct triage reducing the requirement for Tier-2 and Tier-3 analysts. This is important considering the cybersecurity skills gap previously outlined. Further, layering Machine Learning (ML) and Artificial Intelligence (AI) capabilities into the *R augmented SOC can provide better analysis capabilities and visibility across the enterprise. The following are the benefits of a Virtual SOC capability:

- Cost reduction for SOC maintenance;
- Ability to monitor varied sources and facilitate endpoint analysis;
- Identify security improvements in the enterprise ecosystem;
- Improving business-level stakeholder understanding and awareness;
- Integrated augmented intelligence and tipping and queuing for network events and mitigating potential threats;
- Augment data visualization; improve forecasting, analysis; and decision-making [14].

Additionally, research into the efficacy of using *R technologies to train digital forensic professionals has been conducted with scenarios to obtain evidence from crime scenes in a forensically sound manner [13]. This involved setting up a physical and virtual lab for a variety of situations including imaging flash drives, collecting media, and other activities.

V. Current Solutions

Although *R technologies for cybersecurity are limited in both scope and scale, some solutions address Cybersecurity Awareness Training, Cybersecurity Technical Training, and Cybersecurity Operations.

*A. *R Solutions for Cybersecurity Awareness Training*

CybAR is an Augmented Reality application designed with 20 tasks designed to challenge and engage users by providing interactive answers and feedback on topics such as phishing, ransomware, WiFi security, password creation, data protection, file backups, and social media best practices based on Technology Threat Avoidance Theory (TTAT) [17]. The application is designed to integrate new content into the platform to expand the content repository or increase the technical difficulty.

*B. *R Solutions for Cybersecurity Technical Training*

The Cyberinfrastructure Security Education for Professionals and Students (CiSE-Pros) provides a cybersecurity training program integrating aspects of physical security. The application provides a user tutorial, for entering and exiting a data center, interacting with and inspecting hardware components within the data center, and replacing defective hardware components [19]. Although limited in scope, this application demonstrates how physical security elements can be integrated with other aspects of cybersecurity training including clean desk policies, access control, securing physical documents, securing desktops, and various other opportunities.

*C. *R Solutions for Cybersecurity Operations*

The Virtual Reality Data Analysis Environment (VRDAE) is a beta application to provide cybersecurity analysts with a collaborative environment and data visualization tools to depict linkages between nodes within an enterprise environment [20]. Additionally, there is an integrated Visual Intrusion Detection System (VIDS) developed to address the proper design and implementation of computer networks and the associated traffic and alert data. The additional benefit of this capability is that it provides future research on how users interact with the data within a virtual environment. A third tool is a Virtual Data Explorer (VDE) which presents users with stereoscopically perceivable data visualizations capable of viewing the functional topology of a set of computer networks and associated nodes [20].

Viewpoint is a technology that allows humans to interact with data using mixed reality interfaces and consumes vast amounts of data to create an analysis capability for cybersecurity risk and operations [21]. The tool uses metadata from network appliances to create a visualization of activity while layering information from multiple sources to create a simulation of the enterprise network and traffic. Additionally, users can interact with the simulation to create attack maps and generate intrusion models, remediate breaches, and develop attack signatures [21]. The utility patent describes the tools as, "The network security monitoring and correlation system utilizes mixed reality techniques to display contextual and prioritized data visualization schemes, thereby allowing a human analyst to quickly inspect and understand the environment surrounding computer hosts within a monitored network [22]."

VI. Gaps in Research

A. *R Framework for Cybersecurity Training

There is no clearly defined framework available for integrating *R technologies into cybersecurity training. However, current research and development of gamification for cybersecurity training can be adapted to *R technologies considering those technologies can be thought of as an extension of gamification. Cybersecurity Awareness is impacted by developing capability and behavior. Capability includes the knowledge, skills, and abilities users need. Behavior deals with the actions and attitudes of users. Although capability and behavior may not directly impact each other, there are indirect influences that impact users. These concepts are depicted in Figure 2 [18]. Further, Tables 1 and 2 provide an overview of gamification mechanics and requirements for a cybersecurity awareness training framework.

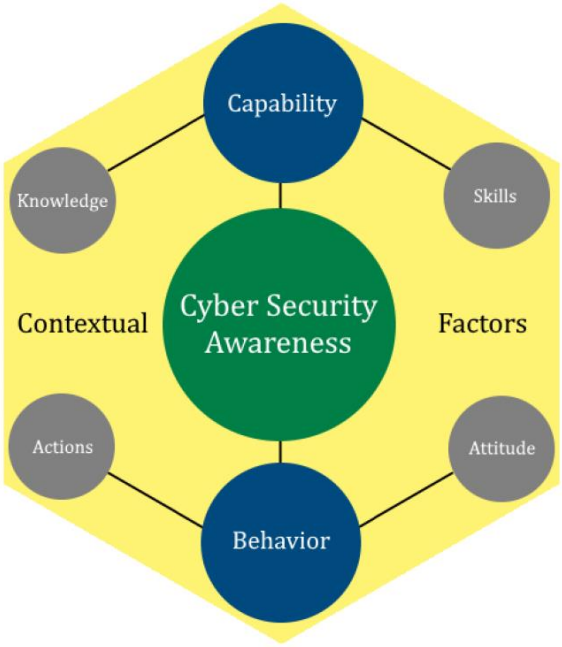


Figure 2 – Cybersecurity Awareness Constructs [18]

Categories	Gamification Mechanics
Cooperation / Competition	- Leaderboards - Social - Guilds - Roles - Avatars - Virtual Goods
Prizes	- Badges / Medals - Trophies - Achievements - Awards, Trading, Gifting / Rewards
Adventures	- Challenges - Actions - Quest / Goal / Mission - Boss Battles
Progression	- Progress Bar / Status - Points / XP - Levels - Feedback / Reports
Surprises	- Unlockable Content - Easter Eggs - Lottery / Game of Chance - Notifications

Table 1 – Gamification Mechanics [18]

Categories	Requirements
Cybersecurity Awareness (CSA)	- Establish business targets and learning objectives - Distinguish relevant topics and content regarding learning objectives - Make sure the content is recognizable and relevant for participants - Perform continuous monitoring; check content's relevance and up to date
Gamification	- Identify motivations of participants to align gamification tactics (ARCS+G) - Apply different gamification concepts to appeal to different participants - Make sure the gamification concepts align with the objectives
Additional	- Perform an analysis of cultural and lifestyle differences that might affect training experiences and results - Adopt a flexible approach; possibilities to change or adjust models - Enable customization. e.g. to different users, message to be delivered, or content - Offer different delivery methods, e.g. print for complex information - Provide short sessions on a regular basis to improve retention

Table 2 – Framework Requirements [18]

B. Qualitative / Quantitative Research on *R Training Effectiveness

Evidence for the effectiveness of commercial and educational game based learning while leveraging immersive technologies has been exceedingly positive. Game-based and interactive learning content is typically more engaging and immersive for the learner. It has been shown to provide meaningful interactions between the learner and the content producing a high level of transferrable skills to the physical world. Additionally, these learning modalities have shown increased cognitive, perceptual, affective, motivational, and behavioral results.

The availability of qualitative and quantitative research on leveraging *R technologies for cybersecurity training, education, and awareness is nearly non-existent. Various studies have been conducted on the efficacy of *R training for STEM education and sociological uses. These studies focus on survey participants from various points in their academic and

professional careers. The research reviews the use of *R technologies from similar perspectives. Equipment availability, equipment comfort, costs (equipment, content development, offset of physical assets), user experiences (availability, realism, interactivity), and safety are consistent criteria across research studies regardless of the discipline or use case.

Due to the lack of cybersecurity-specific research on the effectiveness of *R technologies in cybersecurity, research was evaluated from different use cases and disciplines which provide a solid foundation and understanding which can be used to guide future research.

VR Education Model

Cooper and Thong [25] describe Virtual Reality as a transformational tool and describe the VR Education Model (VEM) as inclusive of terms such as experiencing, engagement, equitability, and everywhere.

- Experiencing includes the ability for the learner to experience things from various locations, such as space, or phenomena from various historical times or locations. Additionally, the same phenomena from their point of view (POV) or that of another learner.
- Engagement is indicated by the learner's attention, novelty, interest, feedback, and challenge across the spectrum of emotional, sensory, and spatiotemporal criteria.
- Equitability refers to stakeholder actions and environments that promote great consistency in the educational experience. Additionally, physical experiences available to those in certain geographic locations or areas of affluence may be replicated in virtual reality to provide opportunities for all students with access to the technology. Further, VR could homogenize cohorts of students using avatars removing certain biases from social interaction.
- Everywhere identifies that VR can provide Collaborative Learning Environments (CVEs) for learners to collaborate globally to solve problems. This experience provides the ability to learn anywhere at any time with collaborators from around the world which would not be possible or restricted by other learning modalities.

Education Case Studies

These aspects are complemented by the research conducted by Steffen, Gasking, Meservy, Lenkins, and Wolman [26] which provide a framework for various affordances for VR and AR technologies correlated with specific aspects outlined as:

- Diminish negative aspects of the physical world
  - Reduce physical risk
  - Reduce emotional/mental risk
- Enhance positive aspects of the physical world
  - Increase empathy
  - Amplify reality
  - Coordination
  - Collaboration
  - Communication
  - Enhanced computing
  - Facilitate information
  - Filter information
- Recreate existing aspects of the physical world
  - Video logging
  - Mobile computing
  - Understand proximal positioning
  - Physical interaction with digital objects
  - Training
  - Reduce resource cost
  - Enable physically incapable participants
- Create aspects that do not exist in the physical world
  - Depict the nonexistent
  - Overcome space-time linearity

Their team conducted two case studies to identify the extent Physical Reality, Augmented Reality, and Virtual Reality impact the following:

- Reduce physical risk
- Reduce emotional/mental risk
- Obtain useful additional information not available by default
- Highlight, filter, or block certain information
- Reduce costs associated with time, effort, or financial resources
- Participate in an activity that would otherwise be impossible for me
- Gain access to objects, activities, or environments that existed in the past or have not yet come into existence (time constraints)
- Experience the breadth and depth of detailed sensory inputs
- Leverage important details in my immediate physical surroundings (within the scenario) [26]

Study 1 was an experiential survey conducted at a large, private university. Study 2 expanded and complemented Study 1 by providing participants with a wider variety of *R technology. The results of these studies are captured in Figures 3 and 4.

	Mean			Std Dev			Significantly different?		
Affordance/Modifier	AR	VR	PR	AR	VR	PR	AR-VR	AR-PR	VR-PR
Reduce Physical Risk	7.90	8.81^{H}	2.07^{L}	2.15	1.78	1.94	p < .001	p < .001	p < .001
Reduce Emotional/Mental Risk	6.79^{VA}	7.23^{VA}	2.94^{L}	2.04	2.00	2.30	p = .062	p < .001	p < .001
Facilitate Additional Info	7.65^{VA}	7.36^{VA}	4.15^{L}	1.70	2.03	2.92	p = .420	p < .001	p < .001
Filter Info	8.15^{H}	7.12	2.75^{L}	1.76	2.25	2.18	p < .001	p < .001	p < .001
Reduce Resource Costs	7.56	7.96^{H}	3.03^{L}	1.64	1.72	2.18	p < .050	p < .001	p < .001
Enable Physically Incapable Participant	7.65	8.93^{H}	2.07^{L}	1.89	1.38	2.55	p < .001	p < .001	p < .001
Depict the Nonexistent	7.72	8.43^{H}	2.44^{L}	1.72	1.83	2.96	p < .001	p < .001	p < .001
Overcome Space-time Linearity	7.69	8.82^{H}	1.33^{L}	1.82	1.47	1.98	p < .001	p < .001	p < .001
Importance of Sensory Vividness	4.16	3.07^{L}	9.46^{H}	2.78	2.65	1.28	p < .001	p < .001	p < .001
Importance of Physical Context	6.53	4.01^{L}	7.60^{H}	2.65	2.99	2.45	p < .001	p < .001	p < .001

Notes: ^{H} Highest mode for affordance/modifier; ^{L} Lowest mode for affordance/modifier; ^{VA} VR/AR are not statistically different from each other.

Figure 3 – Study 1 Statistics [26]

	Mean			Std Dev			Significant difference		
Affordance/Modifier	AR	VR	PR	AR	VR	PR	AR-VR	AR-PR	VR-PR
Reduce Physical Risk	6.95	7.69^{H}	5.65^{L}	2.48	2.37	3.33	p < .050	p < .001	p < .001
Reduce Emotional/Mental Risk	6.16^{VA}	6.75^{VA}	5.39^{L}	2.72	2.63	3.20	p = .110	p < .050	p < .001
Facilitate Additional Info	7.71^{VA}	7.36^{VA}	6.11^{L}	2.02	2.22	2.83	p = .410	p < .001	p < .001
Filter Info	7.43^{VA}	7.00^{VA}	4.68^{L}	2.24	2.65	3.28	p = .330	p < .001	p < .001
Reduce Resource Costs	7.28^{VA}	7.16^{VA}	5.42^{L}	2.21	2.36	2.98	p = 1.00	p < .001	p < .001
Enable Physically Incapable Participant	7.10	8.25^{H}	4.31^{L}	2.30	2.03	3.54	p < .001	p < .001	p < .001
Depict the Nonexistent	6.99	8.07^{H}	4.46^{L}	2.18	1.99	3.49	p < .001	p < .001	p < .001
Overcome Space-time Linearity	6.88	8.05^{H}	4.24^{L}	2.44	1.96	3.60	p < .001	p < .001	p < .001
Importance of Sensory Vividness	5.52^{L}	5.66	7.46^{H}	2.94	3.07	2.73	p = 1.00	p < .001	p < .001
Importance of Physical Context	7.25^{H}	6.48^{VP}	6.52^{VP}	1.99	2.68	2.82	p < .050	p < .050	p = 1.00

Notes: ^{H} Highest medium for affordance/modifier; ^{L} Lowest medium for affordance/modifier; ^{VA} VR/AR aren't statistically different from each other; ^{VP} VR/PR aren't statistically different from each other.

Figure 4 – Study 2 Statistics [26]

STEM / Physical Systems

Skorenkyy, Kozak, Zagorodna, Kramar, and Baran developed a conceptual model to map AR-assisted scenarios onto competency frameworks using an agricultural cyber-physical system component [24]. Their work outlined the components (cybernetic, network, physical), realization (applications, services, protocol interfaces, sensors, actuators), and requirements (security, interoperability, dependability, real-time and streaming data, predictability, sustainability) functional requirements for cyber-physical systems (Figure 5). They mapped these requirements to the NICE framework of building blocks for a capable and ready cybersecurity workforce (Figure 6). And finally introduced the concept and scenario game development model for a cybersecurity training project (Figure 7). This work is relevant to the lack of content and engagement for users. It also provides a foundation for future content development.

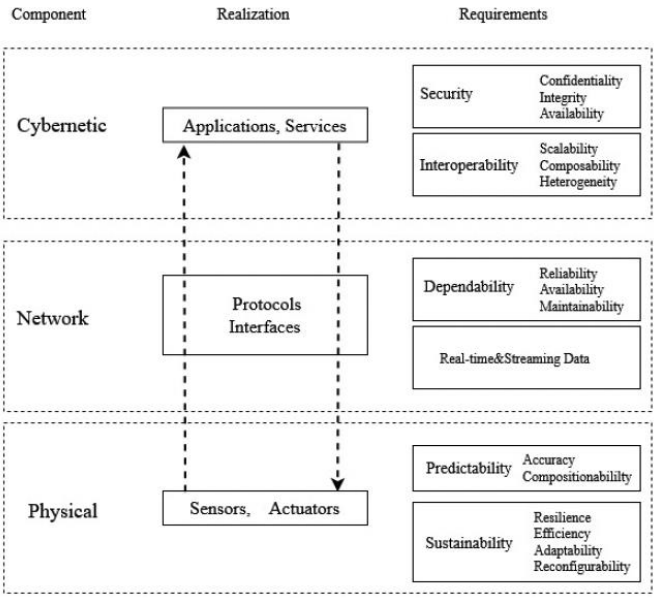


Figure 5 – Functional Requirements of Cyber-Physical System Realizations [24]

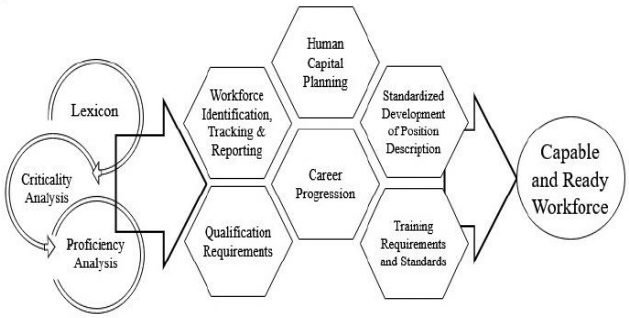


Figure 6 – NICE Framework of Building Blocks [24]

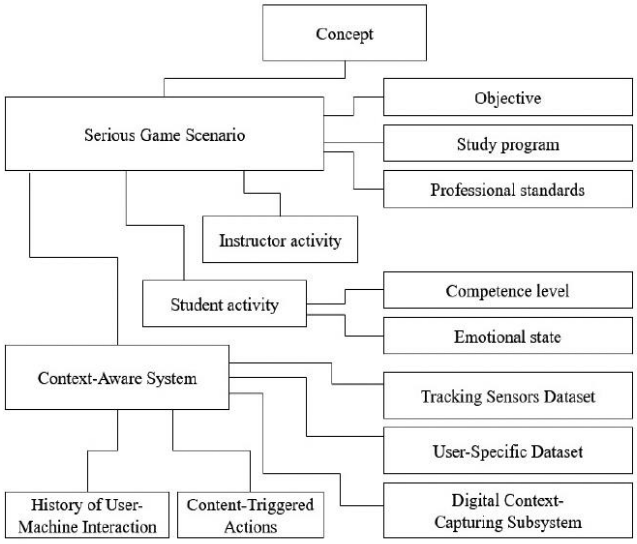


Figure 7 – Game Scenario Model for Cybersecurity Training [24]

Related to the Skorenkyy et al work, Jones and Golub [27] developed two prototype VR experiments to evaluate the efficacy of VR technologies in STEM education. The first replicated a Resistor-Inductor-Capacitor (RLC) circuits lab. The second was used to simulate the investigation of tensile strengths and stress-strain response in different materials. The Likert scale survey results from the study are outlined in Figure 8.

Question	Average	Mode	Standard Deviation
I was comfortable wearing the Head Mounted Display	4.17	4	0.37
The detail of the Virtual Reality Equipment was sufficient that I could recognize similar equipment in a real-life lab.	4.67	5	0.47
The actions needed to perform the Virtual Reality lab was similar enough to a real-life lab such that I could perform a similar real-life lab	3.83	4	0.89
The Virtual Reality lab would encourage experimenting with the equipment	4.5	5	1.1
Overall, I feel that a Virtual Reality lab would be an effective way to learn laboratory topics.	4.83	5	.37

Figure 8 – Jones Golub Likert Scale Survey and Results [27]

Engineering Education and Professional Training

Research from Udeozor, Toyoda, Abegao, and Glassey highlights multiple applicable criteria for our study including highly technical content, developing transferrable skills, and safety [28]. Their research leverages the Unified Theory of Use and Acceptance of Technology (UTAUT2) framework which was developed to predict technology acceptance. This framework theorizes that Performance Expectancy (PE), Effort Expectancy (EE), Social Influence (SI), Facilitating Conditions (FC), Hedonic Motivation (HM), Price Value (PV), and Habit (H) determine technology use intentions. A modified framework (Figure 9) was used for their study.

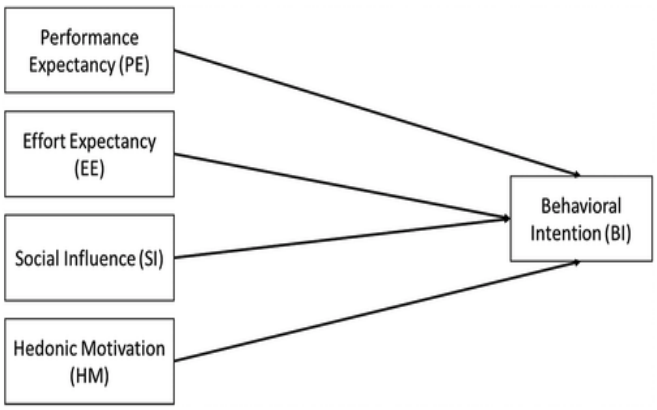


Figure 9 – Modified UTAUT2 Model

Their research provided both quantitative and qualitative results both correlating towards the acceptance and willingness to adopt this technology for education and training from the student perspective (research question 1) and the employee perspective (research question 2). Specifically, the mean scores of students on all constructs measured from 3.6 to 4.8 with HM and EE having the highest mean scores [28]. Additionally, students scored high on the BI construct which indicates enthusiasm towards adoption. Similarly, the researchers used two open-ended questions in their study.

1) *Why do you think using Immersive Virtual Reality (IVR) games for H&S education could be a good idea?*
2) *Why do you think using IVR games for H&S education could be a bad idea?*

Themes from Question 1 include the opinion that IVR games could enhance learning and retention, improve safety in training, and cost benefits. Themes from Question 2 include cost, the challenge of game design, gameplay distractions, the ineffectiveness of games, and lack of acceptance by students and teachers. The results for employees were slightly higher with mean scores averaging between 3.8 to 5.1 with PE and EE having the highest mean scores at 5.0 and 4.8 respectively [28]. The implications of their study are:

- IVR games should be fit for the purpose
- Finding the right balance between quality of immersion, representation, and fidelity when designing content is important
- IVR games and similar pedagogical tools should be used to complement existing pedagogies rather than stand-alone
- Students can be encouraged to be co-designers of games.
- Integrating debriefing sessions into the learning activities would be beneficial [28].

C. Limited Content and Simulations

Although the research on *R technology for cybersecurity is lacking, research has been conducted on leveraging gamification strategies for cybersecurity awareness and training. The results of these studies could guide future research in *R technology adoption, use, and effectiveness in cybersecurity. This section will evaluate a few examples which highlight basic gamification for a specific knowledge area using a role-playing game theme, an augmented reality tool covering a wide spectrum of cybersecurity awareness domains, and a Virtual Reality (VR) First-Person game that puts the learner in an IT technician role.

Role Playing Game (RPG)

Scholefield and Shepherd conducted an exploratory study on the use of gamification to educate users on a specific task of password security [29]. They identified that previous gamification was focused on younger audiences and high school students using browser-based applications. They postulated that this limited reach since cybersecurity awareness impacts everyone and browsers are not as accessible as other

platforms. To overcome the second concern, they developed their platform using a unity role-playing quiz application for Android which maintained 75% of the market share. The results of the study indicated that a majority of participants agreed that the password security game helped increase their knowledge on password security, found it enjoyable, and considered gamification an effective method for teaching computer security (Figures 10, 11, 12, 13).

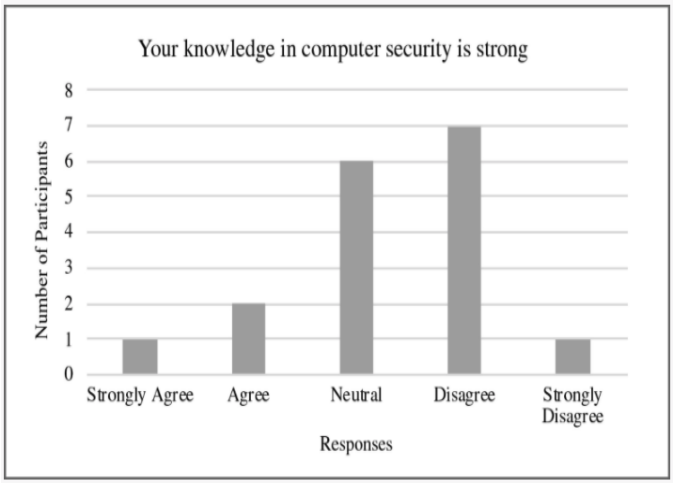


Figure 10 – Self-Reported Security Knowledge [29]

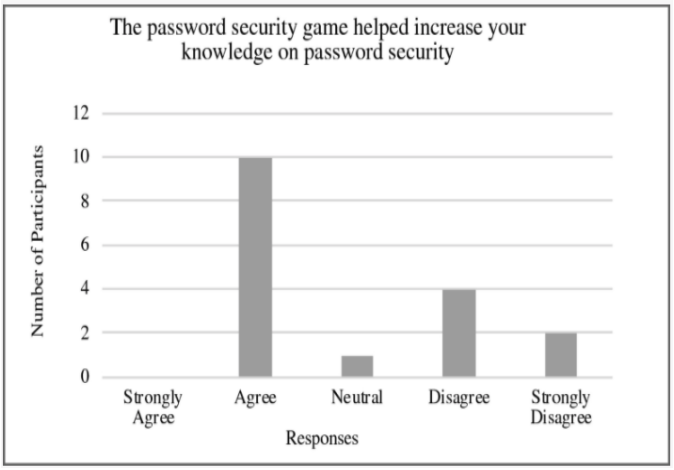


Figure 11 – Knowledge improvement [29]

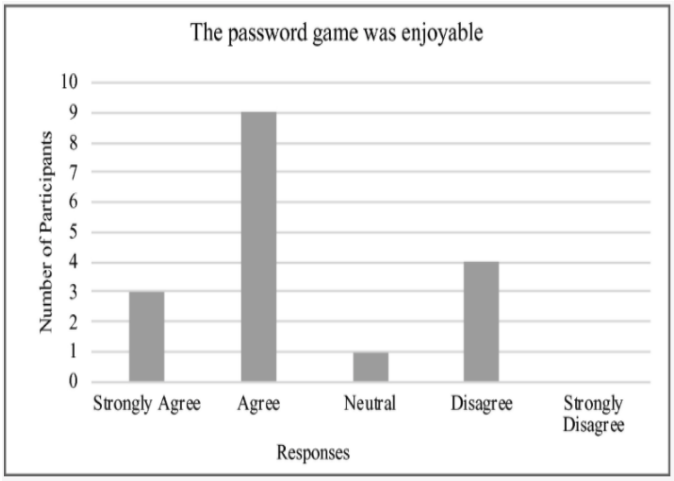


Figure 12 – Enjoyment [29]

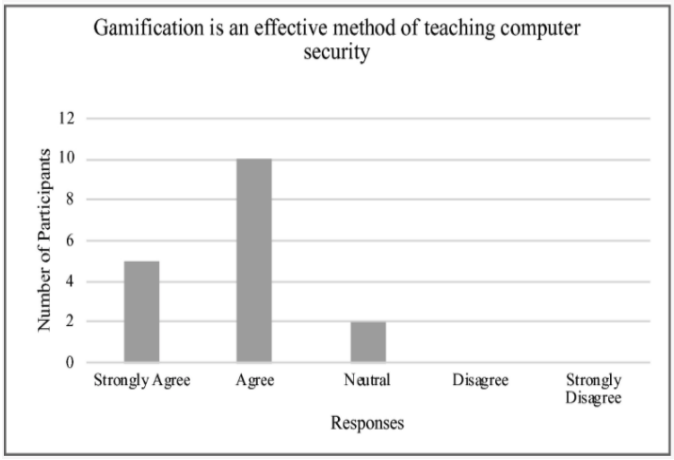
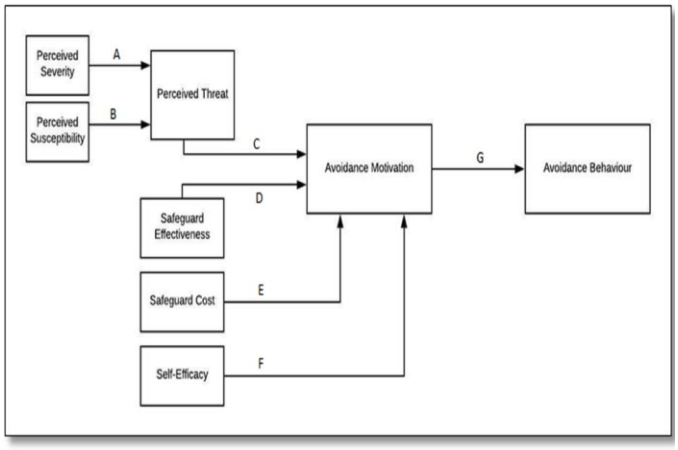


Figure 13 – Effectiveness [29]

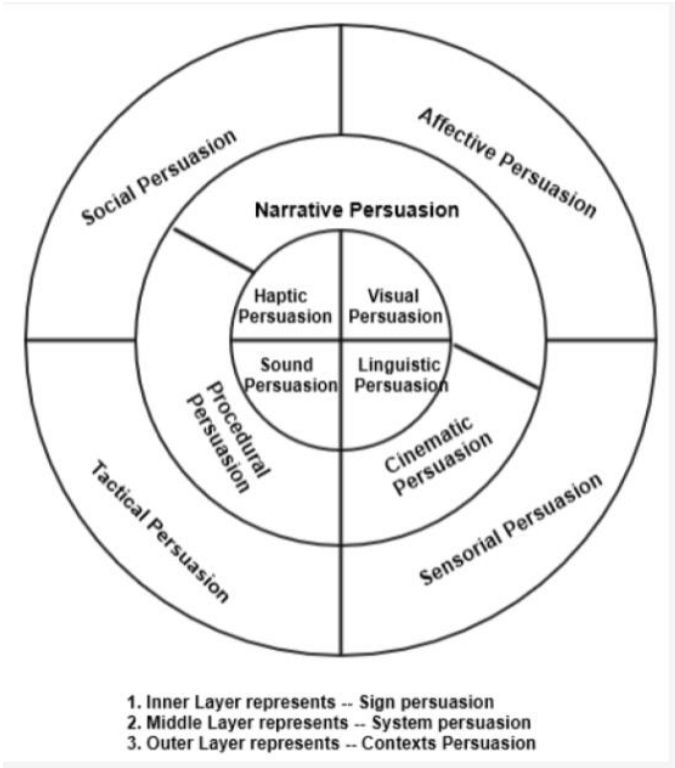
Augmented Reality (AR) Game

Alqahtani and Kavakli-Thorne evolved the simple role-playing game by developing an Augmented Reality game for Cybersecurity Awareness (CybAR) [17]. Their experience focused on high-level user behavior across the spectrum of cybersecurity including spoofed emails, SMS phishing, scam phone calls, identity theft, ransomware, and phishing through social media [30]. They leveraged elements of the Technology Threat Avoidance Theory (TTAT) to develop their game framework (Figure 14) and the Condepumpido knowledge model (Figure 15).



A - Perceived severity has a positive interaction with Perceived threat
B - Perceived susceptibility directly affects Perceived threat
C- Perceived threat motivates the users to avoid them
D & E - Effectiveness of safeguard and cost of safeguard are important elements for motivating users for adopting avoidance mechanism
F - Self-confidence for taking threat measures motivate users for adopting avoidance mechanism
G - Users' avoidance motivation leads to their avoidance behavior, which is taking safeguarding measures to reduce the threat.

Figure 14 – CybAR Game Design Framework [17]



1. Inner Layer represents -- Sign persuasion
2. Middle Layer represents -- System persuasion
3. Outer Layer represents -- Contexts Persuasion

Figure 15 – CybAR Knowledge Model [17]

The researchers found that more than 90% of participants (91 participants) agreed that the CybAR game was an effective method of learning cybersecurity-related concepts, helped the user learn about cybersecurity attacks from mistakes, was a fun method of learning cybersecurity, motivated the user to learn more about cybersecurity, was easy to understand and play, mimicked real-life cybersecurity scenarios in a presentable way, and were motivated to use CybAR in the future (Figure 16).

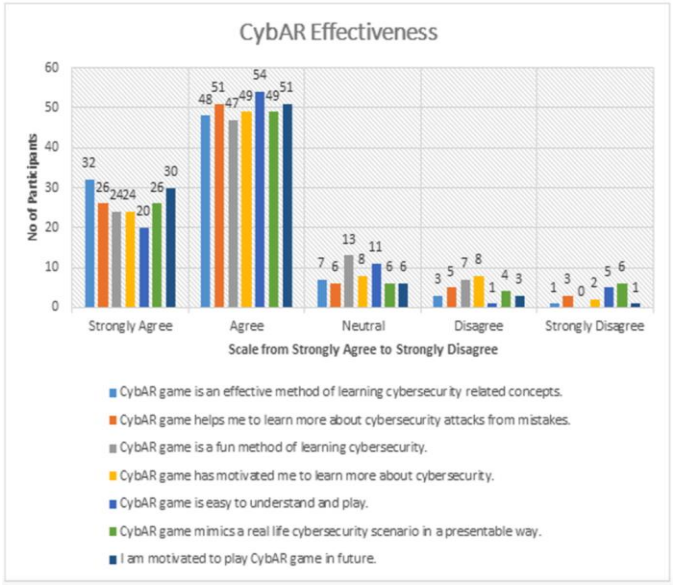


Figure 16 – CybAR Effectiveness [17]

Virtual Reality (VR) Game

Veneruso, Ferro, Marrella, Mecella, and Catarci researched the effectiveness of a Virtual Reality (VR) experience called CyberVR. This game placed the user into an IT technician role who completes mini-games that cover relevant and contemporary topics in cybersecurity [30]. Their game consists of two levels. The first is an orientation level for the learner. The second level focuses on skills development in network mapping/scanning, information flow, code injection, patch management, dynamic software analysis, privilege escalation, and public-key cryptography. Their research focused on validating the following:

- H1 - Traditional textbook learning increases users' awareness of cybersecurity issues.
- H2 - Playing CyberVR increases users' awareness of cybersecurity issues.
- H3 - Learning through CyberVR is more engaging than traditional textbook learning [30].

The researchers concluded that CyberVR is equally, and in some cases, more effective as a learning method toward cybersecurity education than traditional textbook learning and that CyberVR is more engaging as a learning method toward cybersecurity education than traditional textbook learning [30].

VII. *R Adoption Challenges

Adopting any emerging technology comes with a variety of challenges. One of the ongoing challenges with *R technologies is locomotion within the simulated environment. This can significantly impact the user's willingness to leverage *R technologies, may reduce the realism of training, and may reduce training effectiveness. This limitation is caused by the restrictions imposed by sensors, the range of communication

between wearable technology and the simulator, and the field of view associated with the headsets [19].

There are many barriers to adoption regarding *R technologies for education, training, and operational usage. These barriers include the potentially high financial costs of acquiring the hardware; the lack of realism, fidelity, and skill transfer issues; physical effects on end-users; no curriculum content; and the requirements for a mobile device. These adoption challenges will be explored from the K-12 educational perspective, higher education, and organizations.

Public K-12 schools, which account for nearly 87% of students, continuously face funding concerns, and has become more pronounced due to the COVID-19 pandemic. This aligns with the cost being one of the primary barriers for the massive adoption of AR/VR solutions; lack of understanding of the value of VR; and the return on investment for improving education efficacy, retention, and engagement among learners [31]. Compounding this issue is the lack of knowledge about how *R technologies can support education. The best way to understand *R technology is to experience it. This requires explaining how those experiences can improve education. It also requires educators and administrators to agree on the value of the technology. Health concerns also top the list of adoption challenges. Sixty percent of parents are "somewhat concerned" including thirty percent being "very concerned" about VR's negative health effects [31]. Bumping into things, dizziness, nausea, headaches, and eyestrain are among the physical health concerns. Additionally, isolation, emotional, and trauma from scary, violent, or sexually explicit content are additional concerns.

Recent research [32] was conducted to understand the limited adoption of Augmented and Virtual Reality (AVR) technology in higher and tertiary education despite the potential benefits. An important point for this study is the inclusion of AVR-associated Internet of Things (IoT) devices. Table 3 outlines the concerns for AVR technology.

Primary Concern	Associated Concerns
Security Concerns	• Credential Exposure • Cross-Site Scripting (XSS) • SQL Injection • Weak Account Lockout Settings • Insufficient Authentication and Authorization methods
Environmental Concerns	• Heavy Metal Usage • Toxic Chemical Usage • Cost to mine rare metals

Ethical Concerns	• Human Rights
	  • Security
	  • Data Protection
	  • Privacy
	• Responsibility
	  • Punishment
	  • Management
	  • Laws and Regulations
	• Morality

	• Age
	• Culture
	• Experience
	• Mentality
	  • State of Mind
	  • Understanding
	  • Trauma
	  • Tolerance

Content Availability	• Discipline Limitations • Accessibility • Immersion and Interaction

Table 3 – *R Adoption Issues in Higher Education [33]

Organizations face similar adoption issues as educational institutions. There are legal concerns, moral questions, accessibility, privacy and security, and health concerns. Additionally, Martec's Law states that technology changes exponentially yet organizations change logarithmically (Figure 17) [33].

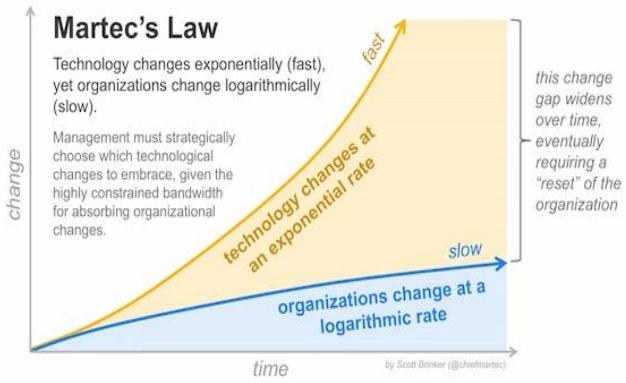


Figure 17 – Martec's Law [33]

Additionally, organizations must face the reality that failing to adopt *R technology could reduce profitability and agility in the marketplace. This is especially true for small businesses that can't afford the technology or where it may not be relevant within their industry vertical. This is an example of where the market may influence adoption which would not influence educational institutions.

Impacting the adoption from all groups is the issue of usability and integration. Integrating operations across virtual reality, augmented reality, and desktop systems is increasingly difficult. Additionally, data ingestion and synchronization across platforms can introduce discrepancies during analysis and operations. Further, usability issues arise based on groups and demographics, specifically the age of the user [23].

VIII. Analysis and Example

Education and training are typically conducted in a few modalities: In-person/face-to-face, Online (synchronous/asynchronous), or some form of hybridization. There are pros and cons for each of these modalities. With each of these, technology continues to support education and

training. COVID-19 has forced educators, trainers, and employers to adopt innovative solutions to continue operations.

Research and application on using *R technologies for education, distance education, training, and operationally is limited holistically and even more so within cybersecurity. Despite this limitation, the research reviewed indicates that *R technology can be used to supplement and enhance current education, training, and awareness campaigns. The various studies identified a positive correlation between using gamification and *R technologies in three primary ways:

- Increase in both knowledge attainment and retention
- *R technologies are effective in delivering content in a realistic and applicable manner
- Increased enjoyment and motivation to learn the content

The information obtained through this research can be distilled into two tables. Table 4 outlines the high-level capabilities, pros, and cons of using *R technologies across disciplines and use cases. Table 5 correlates the specific research to the benefits.

Capabilities	Pros	Cons
Diminish negatives of the physical world	Cost benefits	Security concerns
Enhance positive aspects of the physical world	Reduce physical/ emotional/mental risk	Environmental concerns
Recreate existing aspects of the physical world	Highlight, filter, or block certain information	Ethical concerns
Create aspects that do not exist in the physical world	Ability to leverage or introduce sensory inputs	Content availability
	User engagement, interaction, and enjoyment improved	Physical effects

Table 4 - *R Capabilities, Pros, Cons

Benefit	Research
Skill/knowledge transfer and development	• Alqahtani [17] • Skorenkyy [24] • Steffen [26] • Udeozor [28] • Scholefield [29] • Veneruso [30]
Skill/knowledge retention	• Alqahtani [17] • Steffen [26]
Similarity to real-world experiences (realism)	• Alqahtani [17] • Skorenkyy [24] • Steffen [26]
Enjoyment/engagement/motivation	• Alqahtani [17] • Steffen [26] • Udeozor [28] • Scholefield [29] • Veneruso [30]
Expected effort expended to learn the material	• Udeozor [28]
Equipment comfort	• Skorenkyy [24]

Table 5 – Benefit / Research Mapping

There are many documented reasons that educational institutions and organizations are not adopting *R technologies despite the evidence supporting that user satisfaction, demonstrable improvements in time to learn new content and skills, and retention of those skills are increased. There is consistency between educational institutions at various levels and organizations in different industries for limited adoption. Specifically, these adoption barriers can be generalized as cost, ethical issues, and lack of applicable content.

Overcoming these adoption issues requires developing value propositions for organizations and continued research into the efficacy of these technologies. It will also require that robust and relevant content be developed and distributed. This may require content developers to provide some content for free to engage users and demonstrate the value. Despite the exponential improvements in *R hardware, developers will need to develop a platform that meets most consumer needs and isn't expected to become obsolete within months of purchase. Additionally, some ergonomic issues continue to plague headsets. For example, the fact that headset straps can mess up the user's hair is a simple and common complaint for users. Finally, champions for the technology must introduce it to organizations and consumers to experience it. It is hard to explain a *R experience, yet once someone experiences it there is usually a moment of clarity. Users must know the technology that exists, how the technology will enhance or replace the current methodologies, and why they should adopt the technology.

Networking / Threat Analysis Tool

An early attempt to identify how Virtual Reality technology could enhance education and operations was conducted by the University of Arizona with an NSA sponsored grant. From 2019-2020, P. Wagner from the University of Arizona conducted the initial development of a VR tool, Virtual Exploit Network Offense Management (VENOM) tool, to explore the ability of cybersecurity defenders to view a medium-scale (50+ Node) network associated with a shipping/delivery company (Figure 18). Traffic focusing on the top networking protocols was simulated within the virtual environment. Additionally, simulated network attack traffic was simulated to identify how visualizations could improve Security Operations Center (SOC) identification and understanding of attacks as they traverse the network in the simulated environment. Finally, dashboards (Figure 19) and heads-up displays (Figure 20) were integrated into the environment to provide situational awareness for the

operational environment. The goals of this research were as follows:

- Develop a VR environment depicting a medium business network with simulated traffic for various protocols and attack traffic.
- Determine the efficacy of using this experience to understand networking concepts and attack traffic.
- Determine whether to use a VR tool to enhance SOC operations and attack identification.
- Determine whether to use a VR tool to develop and rehearse offensive operations

Further analysis must be conducted on the cost-effectiveness, viability, overall improvement of using the VENOM tool for education, attack planning, and mission/attack analysis. Scripted attacks in conjunction with actual and relevant data from attacks and recent network intrusions must be integrated into the environment. Group surveys should be developed to conduct a comparative analysis of current options and the enhanced visualization options provided by VENOM.

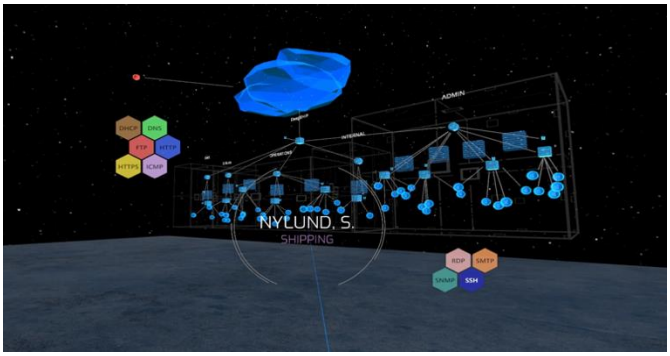


Figure 18 – VENOM Environment

Figure 19 – VENOM Dashboard Example

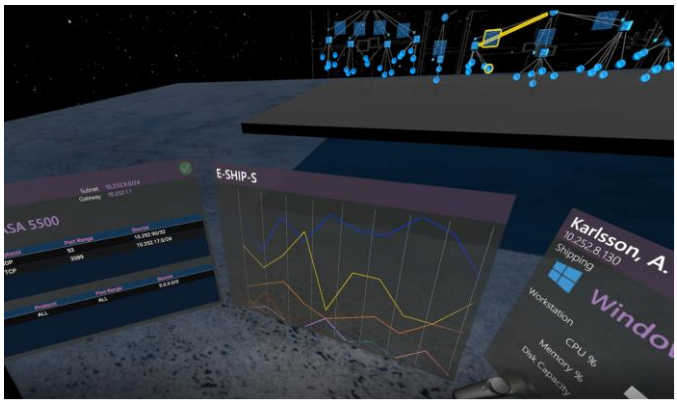


Figure 20 – VENOM Heads-Up-Display Example

IX. Contributions

Contributions of this paper include a table of previous research that identifies how *R technologies can be used for awareness training, technical training, education, and operations for cybersecurity. The table highlights the findings, limitations, and helpful information that could spur future research and development of training content and experiences. Additionally, research consistently demonstrates that there are many uses and positive impacts of *R technologies for cybersecurity. Given the shortage of trained and proficient cybersecurity workers, emerging technologies and creative solutions must be adopted to reduce the cybersecurity workforce gap. Finally, the positive impacts and effectiveness of leveraging *R technologies for cybersecurity purposes were outlined and supported by previous research. This data is important for overcoming the barriers to the adoption of these emerging technologies.

X. Future Research

Virtual Reality has existed for over 50 years. Despite this, research and adoption of this technology is limited. This is especially true for cybersecurity-related issues and adoption. This paper identified a variety of areas that could be researched further. Developing new and innovative hardware and content, technology adoption, or focusing in-depth research on leveraging technology for the areas identified in this paper.

Additionally, several cybersecurity issues related to these technologies were not explored and present excellent research opportunities. As with other technologies, *R technologies gather a variety of data on users. The protection and privacy of this data should be researched. Similarly, the legal aspects of criminal actions conducted within, or via *R technologies should be researched, and laws should be introduced and adopted. For example, causing psychological harm or harassment through *R is not properly addressed in current legislation. Further, *R technologies introduce new attack/threat vectors. Most hardware requires an internet connection, and some connect with smartphone applications and cloud technologies. Understanding these threat vectors and developing mitigation strategies is critical as *R technologies are adopted by individuals and organizations.

XI. Conclusion

Virtual, Augmented, Extended, and Mixed reality (*R) technologies continue to improve and integrate into society in a variety of ways. These technologies span from layering on top of the real environment to complete immersion into a virtual environment. The research and broad use of *R technologies is limited. This is especially true in the cybersecurity discipline across education, training, awareness, and operations domains. The *R solutions currently available provide limited experiences and scenarios to be used, studied, and analyzed. Additionally, the variety of domains or career fields within cybersecurity will continue to limit how *R technologies and content can be developed to support cyber education, training, awareness, and operations. Further, organizational size, industry, and culture will impact whether the adoption of *R will even be adopted.

The table outlining the systematic literature review of distance and online learning modalities with a focus on virtual, augmented, extended, and mixed-reality technologies provide a resource to guide future research. Readers can quickly identify previous research that has been successful and the limitations of those studies to guide efforts to reduce wasted effort and resources. Additionally, the highlighted frameworks, methodologies, and content can further content development and research in that area. Although not included in the literature review, it is evident that certain disciplines have conducted more research into *R technologies than others. There were many research articles within the medical field and very few on cybersecurity.

The COVID-19 pandemic required organizations to adopt technologies to allow for distributed operations. These technologies included digital and contactless payments, remote work, telehealth, online entertainment, robotics, drones, and most applicable to this paper, distance learning. Most of the education and training had to move to some form of distance learning. This allowed for platforms, such as Zoom, to connect people in new and innovative ways. *R technologies were integrated into the distance learning model which led to new opportunities and research into the efficacy of these technologies. Although not a perfect solution, nor currently a complete replacement for traditional learning modalities, the research determined that *R can increase both knowledge attainment and retention, is effective in delivering content in a realistic and applicable manner, and users enjoyed the learning experience and were motivated to use *R technologies to learn the content.

References

[1] R. Watkins, “Addressing the cybersecurity skills gap: Where do we go from here?. Cyberpion. https://www.helpnetsecurity.com/2021/07/13/addressing-cybersecurity-skills-gap/, July 13, 2021.

[2] B. Lundell and J. Oltsik, “The Life and Times of Cybersecurity Professionals in 2021 Volume V,” Enterprise Strategy Group (ESG) and Information Systems Security Association (ISSA) International, https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf, July 2021.

[3] S. Mandal, “Brief Introduction of Virtual Reality & Its Challenges,” International Journal of Scientific & Engineering Research, Volume 4, Issue 4, https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.302.4239&rep=rep1&type=pdf, April 2013.

[4] B. Marr, “What Is Extended Reality Technology? A Simple Explanation for Anyone,” Forbes, https://www.forbes.com/sites/bernardmarr/2019/08/12/what-is-extended-reality-technology-a-simple-explanation-for-anyone/?sh=6fb98c1a7249, August 12, 2019.

[5] A. Awoke, H. Burbelo, E. Childs, D. Manocha, F. Mohammed, N. Rewkowski, and L. Stevens, “An Overview of Enhancing Distance Learning Through Augmented and Virtual Reality Technologies,” arxiv labs, https://arxiv.org/abs/2101.11000, August 9, 2021.

[6] “Beyond hand controllers: The future of interaction in VR/AR,” XR4Work, https://www.xr4work.com/articles/beyond-hand-controllers-interaction-vr-ar, December 3, 2019.

[7] C. Morais, G. Oliveira, J. Teixeira, and A. Torres, “An exploratory study on the emergency remote education experience of higher education students and treachers during the COVID-19 pandemic,” British Journal of Educational Technology, https://doi.org/10.1111/bjet.13112, May 18, 2021.

[8] R. Sobers, “134 Cybersecurity Statistics and Trends for 2021,” Varonis, https://www.varonis.com/blog/cybersecurity-statistics/, March 16, 2021.

[9] M. Madon, “Cybersecurity Breakdown: Improving Workplace Awarenes,” Mimecast, https://www.mimecast.com/blog/cybersecurity-breakdown-improving-workplace-awareness/, December 5, 2018.

[10] R. Watkins, “Addressing the cybersecurity skills gap: Where do we go from here?” Help Net Security, https://www.helpnetsecurity.com/2021/07/13/addressing-cybersecurity-skills-gap/, July 13, 2021.

[11] ISSA, “Cybersecurity Skills Crisis Continues for Fifth Year, Perpetuated by Lack of Business Investment,” Information Systems Security Association (ISSA) International, https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment/, July 28, 2021.

[12] S. Adinolf, R. Altizer, R. Brown, and P. Wyeth, “Towards Designing Agent Based Virtual Reality Applications for Cybersecurity Training,” https://doi.org/10.1145/3369457.3369515, December 2019.

[13] I. Baggili, J. Jacques, and C. Hassenfeldt, “Exploring the Learning Efficacy of Digital Forensic Concpets and Bagging & Tagging of Digital Devices in Immersive Virtual Reality,” Fornsic Science International, https://doi.org/10.1016/j.fsidi.2020.301011, 2020.

[14] M. Hyland and J. Flood, “The Emergence of Virtual Reality and Augmented Reality in the Security Operations Center,” Security Intelligence, https://securityintelligence.com/the-emergence-of-virtual-reality-and-augmented-reality-in-the-security-operations-center/, July, 3, 2017.

[15] N. Li and Y. Zhu, “Virtual and augmented reality technologies for emergency management in the built environments: A state of the art review,” Journal of Safety Science and Resilience, https://reader.elsevier.com/reader/sd/pii/S266644962030030X?token=944A1B3CE4960855AAE338640ACD23F3B13421A45A0EBB957C263FC35118DBC3F27E4A52AA62D54EC9654B5859664576&originRegion=us-east-1&originCreation=20210928141153, 2021.

[16] M. Abdous, W. He, W. Li, and Z. Zhang, “ Cybersecurity awareness training programs: a cost-benefit analysis framework,” Emerald Insight, https://www.emerald.com/insight/0263-5577.htm, January 11, 2021.

[17] H. Alqahtani and M. Kavakli-Thorne, “Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR),” MDPI, https://www.mdpi.com/2078-2489/11/2/121/pdf, February 21, 2020.

[18] I. Rieff, “Systematically applying gamification to Cybersecurity Awareness Trainings: A framework and cast study approach,” Delft University of Technology, https://repository.tudelft.nl/islandora/object/uuid:bf832ca0-91d9-4be1-9a25-fe284c23d115/datastream/OBJ1/download, March 2018.

[19] M. Bruner, D. Chakravorty, N. Gober, D. McMullen, A. Payne, and J. Seo, “Using Virtual Reality to Enforce Principles of Cybersecurity,”

Journal of Computational Science Education, https://doi.org/10.22369/issn.2153-4136/10/1/13, 2019.

[20] K. Kullman, M. Ryan, and L. Trossbach, "VR/MR Supporting the Future of Defensive Cyber Operations," Science Direct, https://doi.org/10.1016/j.ifacol.2019.12.093, 2019.

[21] J. Ingalls, "Viewpoint – Cybersecurity Data Visualization in the Next Dimension," Ingalls Information Security, https://iinfosec.com/viewpoint/, 2021.

[22] J. Ignalls, "Network security monitoring and correlation system and method of using same," Justia, https://patents.justia.com/patent/10965561, August 3, 2016.

[23] J. Kasurinen, "Usability Issues of Virtual Reality Learning Simulator in Healthcare and Cybersecurity," Procedia Computer Science, https://www.sciencedirect.com/science/article/pii/S1877050917324031/pdf?md5=5ea489302c9d2f0bfa2e86ce09dd36c4&pid=1-s2.0-S1877050917324031-main.pdf, 2017.

[24] I. Baran, R. Kozak, O. Kramar, Y. Skorenkyy, and N. Zagoronda, "Use of Augmented Reality-Enabled prototyping of cyber-physical systems for improving cyber-security education," Journal of Physics, https://iopscience.iop.org/article/10.1088/1742-6596/1840/1/012026/pdf, 2021.

[25] G. Cooper and L. Thong, "Implementing Virtual Reality in the Classroom: Envisaging Possibilities in STEM Education," STEM Education: An Emerging Field of Inquriy, https://doi-org.ezproxy2.library.arizona.edu/10.1163/9789004391413_005, 2019.

[26] J. Steffan, J. Gaskin, T. Meservy, J. Jenkins, and I. Wolman, "Framework of Affordances for Virtual Reality and Augmented Reality," Journal of Management Information Systems, https://www.tandfonline.com/action/showCitFormats?doi=10.1080/07421222.2019.1628877, August 4, 2019.

[27] A. Jones and M. Golub, "Effectiveness of Current Generation Virtual Reality-based Laboratories," 2018 ASEE Annual Conference & Exposition, https://peer.asee.org/effectiveness-of-current-generation-virtual-reality-based-laboratories.pdf, June 23, 2018.

[28] C. Udeozor, R. Toyoda, F. Abegao, and J. Glassey, "Perceptions of the use of virtual reality games for chemical engineering education and professional training," Higher Education Pedagogies, https://doi-org.ezproxy2.library.arizona.edu/10.1080/23752696.2021.1951615, July 18, 2021.

[29] S. Scholefield and L. Shepherd, "Gamification Techniques for Raising Cybersecurity Awareness," Intenational Conference on Human-Computer Interaction, https://link-springer-com.ezproxy2.library.arizona.edu/chapter/10.1007/978-3-030-22351-9_13, June 12, 2019.

[30] S. Veneruso, L. Ferro, A. Marrella, M. Mecella, and T. Catarci, "CyberVR – An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues," Association for Computing Machinery (ACM), https://doi-org.ezproxy2.library.arizona.edu/10.1145/3399715.3399860, September 28, 2020.

[31] S. Neelakantan, "Schools Face Barriers to VR Adoption in the classroom," Ed Tech, https://edtechmagazine.com/k12/article/2019/12/schools-face-barriers-vr-adoption-classroom, December 2, 2019.

[32] C. Matsika and M. Zhou, "Factors affecting the adoption and use of AVR technology in higher and tertiary education," Technology in Society Volume 67, https://doi-org.ezproxy2.library.arizona.edu/10.1016/j.techsoc.2021.101694, August 13, 2021.

[33] S. Brinker, "Martec's Law: the greatest management challenge of the 21st century," Chief Martec, https://chiefmartec.com/2016/11/martecs-law-great-management-challenge-21st-century/, November 7, 2016.

[34] J. Engbers, "Security Awareness, Training, and Education – A Learning Continuum," Pratum, https://www.pratum.com/blog/331-security-awareness-training-and-education-learning-continuum, April 6, 2022.

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
E. Childs, F. Mohammad, L. Stevens, H. Burbelo, A. Awoke, N. Rewkowski, and D. Manocha	2021	An Overview of Enhancing Distance Learning Through Augmented and Virtual Reality Technologies	Education	- AR/VR ideal to overcome challenges of student motivation, engagement, and information retention	- AR/VR educational solutions are not mature - Lack of customizable content - Health concerns and comfort	- Outlines distance learning methodologies - Evaluates challenges in distance learning
G. Oliveira, J. Teixeira, A. Torres, and C. Morais	2021	An exploratory study on emergency remote education experience for high education students and teachers during COVID-19 pandemic	Education	- Provides evidence-based recommendations on how higher education institutions can use ICT tools in regular learning environment	- Small samples size - Portuguese speaking countries	- Evaluated educational process, ICT usage, and personal adaption during COVID-19 - Evaluated student and teacher perspectives
Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, and I Baran.	2021	Use of Augmented Reality-enabled Prototyping of Cyber-Physical Systems for Improving Cyber-Security Education	Education	- Mapping AR assisted game scenarios onto competency frameworks to improve learning - Approach for agricultural related education but applicable to other teaching (distance learning, computer-aided design, customer assistance)	- Focused on agriculture	- Functional requirements of cyber-physical system realizations (Cybernetic, Network, Physical) - NICE framework of Building Blocks for a Capable and Ready Cybersecurity Workforce Game Scenario Model for Cybersecurity Training Project

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
A. Jones and M. Golub	2018	Effectiveness of Current-generation Virtual Reality-based Laboratories	Education / Training	- VR equipment was relatable to real-life lab equipment - VR lab was similar to real-life lab to perform similar actions - VR Lab encouraged experimentation with equipment - VR lab an effective way to learn lab topics		- Two prototype VR experiments developed (Resistor-Inductor-Capacitor circuits lab and tensile strength and stress-strain response of materials)
C. Udeozor, R. Toyoda, F. Abegao, and J. Glassey	2021	Perceptions of the use of virtual reality games for chemical engineering education and professional training	Education / Training	- Immersive Virtual Reality (IVR) games would provide a better learning experience - Implementation concerns include cost, challenge of game design, ineffectiveness, lack of acceptance by students and teachers	- Sample size limits robust statistical analysis and results - Students were from chemical engineering programs at two universities so results cannot be generalized to engineering students at large	- Unified Theory of Use and Acceptance of Technology (UTAUT2) Framework
S. Veneruso, L. Ferro, A. Marrella, M. Mecella, and T. Catarci	2020	CyberVR – An Interactive Learning Experience in Virtual Reality for Cybersecurity Related Issues	Education / Training	- CyberVR is effective for learning the cybersecurity aspects covered in the game - CyberVR is more engaging as a learning method toward cybersecurity education than traditional textbook learning	- Potential influence of VR's novelty as a technology - No longitudinal studies	- Links to other tools (CyberCIEGE, PhishGuru, Anti-Phishing Phil, and CyberAware)

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
S. Adinolf, P. Wyeth, R. Brown, and R. Altizer	2019	Towards Designing Agent Based Virtual Reality Applications for Cybersecurity Training	Training	- Thematic (Metaphorical Settings, Literal Settings, and Agent Themes) - Stylistic (Agent Appearance, Agent Behavior, Information Flow, Graphic Style), Mechanical (Mail Manipulation, Analysis, Failure Consequences)		- Purpose of the study was to generate concepts to design a VR based cybersecurity training environment - Training programs in a virtual space do not need to conform to same conventions and limitations of the real world - Uncommon valley effect
C. Hassenfeldt, J. Jacques, and I. Baggili	2020	Exploring the Learning Efficacy of Digital Forensics Concepts and Bagging & Tagging of Digital Devices in Immersive Virtual Reality	Training	- No significant difference for students' scores in tested activities - Physical and virtual training methodologies are viable - Employing VR in this test case is effective and beneficial for scalable training	- Little variation in age groups - Limitations in VR experience time due to trial software version - Trials focused on physical activities	- Digital forensics education background - Physical lab setup - VR lab setup - Pre- and Post-test assessments

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
Y. Zhu and N. Li	2021	Virtual and augmented reality technologies for emergency management in the built environments: A state-of-the-art review	Training	- Pre-emergency Preparedness (Hazard Recognition and Prevention, Safety Training) - Responses During Emergency (Human Evacuation, Search and Rescue) - Post-emergency Recovery (Damage Detection, Building Reconstruction)	- Mixed Reality less studied in emergency management research compared to AR/VR - Medical concerns (dizziness and nausea) - Current VR/AR technologies cannot exactly replicate real world situations - Lack of studies in post-emergency recovery	
J. Kasurinen	2017	Usability Issues of Virtual Reality Learning Simulator in Healthcare and Cybersecurity	Training	- Evaluated no-VR, semi-VR, and full-VR - Simulated scenarios (gain access, steal information, shutdown service, evacuation, damage prevention)	- Usability issues combining VR, AR, Desktop systems	

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
J. Seo, M. Bruner, A. Payne, N. Gober, D. McMullen, and D. Chakravorty	2019	Using Virtual Reality to Enforce Principles of Cybersecurity	Awareness / Training	- Cyberinfrastructure Security Education for Professionals and Students (CiSE-ProS) - Develop high-impact, high immersion opportunities - Reinforce and develop knowledge and skills through exercises - Retaining participant interest - Experience: tutorial, entering/exiting the data center, inspecting the data center, and replacing hardware	- Limited experiences	- Discusses NIST, NICE, Certifications - Pedagogy (new experiences, processing ideas and taking ownership of ideas, Opportunities to develop hypotheses to solve problems and validate them
Z. Zhang, W. He, W. Li, and M. Abdous	2020	Cybersecurity Awareness training programs: A cost-benefit analysis framework	Awareness	- Invest wisely in Cybersecurity Awareness Training (CSAT) programs - Make CSAT Programs effective - Identifying CSAT focuses properly - Developing CSAT programs jointly	- Limited by its theoretical basis - Doesn't consider overall cybersecurity costs	- Cost analysis for integrating VR/AR technology

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
H. Alqahtani and M. Kavakli-Thorne	2020	Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness	Awareness	- CybAR game is an effective method of learning cybersecurity related concepts - CybAR game helped learn more about cybersecurity attacks from mistakes	- Experimental study with small sample size - Need to include long-term evaluation regarding knowledge retention - Game improvement	- Game design framework - Knowledge Model
S. Scholefield and L. Shepherd	2019	Gamification Techniques for Raising Cyber Security Awareness	Awareness	- Gamification is an effective method of teaching computer security - Game helped increase knowledge of password security	- Exploratory Study - Small sample size - No long-term evaluation	- Unity role-playing quiz application for Android Platform
I. Rieff	2018	Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and cast study approach	Awareness	- Highlights that behavior and contextual factors are key parts of cyber security awareness - Gamification concepts for the purpose of raising cyber security awareness through training established - Developed a framework for gamifying cybersecurity awareness training	- Literature has expanded since this article but identifies that literature for gamification on cyber security awareness trainings - Theories derived from literature studies might not always reflect current practices or recent trends - Assumptions may need to be researched and validated	- Evaluation framework graphic

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
K. Kullman, M. Ryan, and L. Trossbach	2019	VR/MR Supporting the Future of Defensive Cyber Operations	Operations	Tools - Virtual Reality Data Analysis Environment (VRDAE) - Virtual Intrusion Detection System (VIDS) - Virtual Data Explorer (VDE)	- Need structured evaluation of visualizations - Requires research to understand how generalizable the data shapes over different types of networks, cyber options, and analyst training are - Requires research on operator performance in 3D environments	
J. Ignalls	2021	Viewpoint: Cybersecurity Data Visualization in the Next Dimension	Operations	- Leverages metadata available from enterprise network appliances and other sources - layers information from multiple sources - Event path maps	- Vendor proprietary product with limited access to information	
J. Steffen, J. Gaskin, T. Meservy, J. Jenkins and I. Wolman	2019	Framework of Affordances for Virtual Reality and Augmented Reality	Adoption	- Describes features of Virtual / Augmented / Physical realities and association user adoption - Affordances (user goals, relatively generalizable and constant across implementations, facilitate examining VR and AR in comparison to physical reality)		- Summary of features of VR, AR, and Physical Reality (Features, Advantages, Disadvantages)

Appendix 1

Authors	year	Title	Category	Main Findings	Limitations	Additional Information
S. Neelakantan	2019	Schools Face Barriers to VR Adoption in the Classroom	Adoption	- Costs - Knowledge about what VR is - Effect of technology on children (health and emotional concerns)		
C. Matsika and M. Zhou	2021	Factors affecting the adoption and use of AVR technology in higher and tertiary education	Adoption	- Concerns (Security, Environmental, Ethical, Content Availability) - AVR technology would enable accomplishment of teaching and learning tasks more quickly - Using AVR technology would improve the teaching and learning performance - Using AVR technology in teaching and learning would increase productivity - Using AVR technology would enhance the effectiveness of the teaching and learning process - Using AVR technology would make it easier to conduct teaching and learning	- Develop framework to propel adoption of AVR initiatives - Future work on how emerging / disruptive technologies can be integrated to attain national goals	- Technology Acceptance Model (TAM) - Cost Benefit Analysis and Financial Investment

Appendix 1

AUTHORS	YEAR	TITLE	CATEGORY	MAIN FINDINGS	LIMITATIONS	ADDITIONAL INFORMATION
S. BRINKER	2016	MARTEC'S LAW: THE GREATEST MANAGEMENT CHALLENGE OF THE 21ST CENTURY	ADOPTION	- TECHNOLOGY CHANGES EXPONENTIALLY (FAST), YET ORGANIZATIONS CHANGE LOGARITHMICALLY (SLOW) - GAP BETWEEN TECHNOLOGY CHANGE AND ORGANIZATIONAL ADOPTION WIDENS OVER TIME REQUIRING AN ORGANIZATION RESET	- INDUSTRY STUDY	- MARTEC'S LAW