information

Article

Understanding User Behavior for Enhancing Cybersecurity Training with Immersive Gamified Platforms

Nikitha Donekal Chandrashekar [1], Anthony Lee [2], Mohamed Azab [3,*] and Denis Gracanin [1]

[1] Department of Computer Science, Virginia Tech, Blacksburg, VA 24061, USA; nikitha@vt.edu (N.D.C.); gracanin@vt.edu (D.G.)
[2] Department of Computer Engineering, Virginia Tech, Blacksburg, VA 24061, USA; leean1@vt.edu
[3] Department of Computer and Information Sciences, Virginia Military Institute, Blacksburg, VA 24061, USA
* Correspondence: azabmm@vmi.edu

Abstract: In modern digital infrastructure, cyber systems are foundational, making resilience against sophisticated attacks essential. Traditional cybersecurity defenses primarily address technical vulnerabilities; however, the human element, particularly decision-making during cyber attacks, adds complexities that current behavioral studies fail to capture adequately. Existing approaches, including theoretical models, game theory, and simulators, rely on retrospective data and static scenarios. These methods often miss the real-time, context-specific nature of user responses during cyber threats. To address these limitations, this work introduces a framework that combines Extended Reality (XR) and Generative Artificial Intelligence (Gen-AI) within a gamified platform. This framework enables continuous, high-fidelity data collection on user behavior in dynamic attack scenarios. It includes three core modules: the Player Behavior Module (PBM), Gamification Module (GM), and Simulation Module (SM). Together, these modules create an immersive, responsive environment for studying user interactions. A case study in a simulated critical infrastructure environment demonstrates the framework's effectiveness in capturing realistic user behaviors under cyber attack, with potential applications for improving response strategies and resilience across critical sectors. This work lays the foundation for adaptive cybersecurity training and user-centered development across critical infrastructure.

Keywords: cybersecurity; user behavior; extended reality; digital twin; training; simulation

Citation: Donekal Chandrashekar, N.; Lee, A.; Azab, M.; Gracanin, D. Understanding User Behavior for Enhancing Cybersecurity Training with Immersive Gamified Platforms. *Information* **2024**, *15*, 814. https://doi.org/10.3390/info15120814

Academic Editors: Yang-Wai Chow, Nan Li and Chau Nguyen

Received: 13 October 2024
Revised: 19 November 2024
Accepted: 19 November 2024
Published: 18 December 2024

1. Introduction

Cyber systems are essential, interconnected frameworks that support digital communication, data processing, and information management across sectors like cybersecurity, artificial intelligence, and cloud computing [1]. Their integration into daily life has transformed how individuals work, communicate, and interact, resulting in the widespread use of smart devices, social media, and e-commerce platforms. However, as cyber systems become more embedded in human activities, they face increased vulnerability to attacks, which can lead to severe consequences, such as financial loss, data breaches, and threats to national security. Cyber attacks on critical infrastructure, such as power grids and healthcare systems, pose additional risks to public safety, underscoring the pressing need for robust cybersecurity measures [2].

Cybersecurity is a broad discipline encompassing tools, policies, and risk management approaches designed to protect information and users from various forms of harm. Effective measures are essential for maintaining the integrity, confidentiality, and availability of data and systems, ensuring the stable operation of digital infrastructures [3]. Technical defenses like firewalls and intrusion detection systems (IDSs) are crucial for perimeter security, preventing unauthorized access and reducing exposure to potential threats [4,5]. However, these defenses alone are not sufficient, as human interactions with cyber systems create

vulnerabilities that technical measures cannot fully address. Users can unknowingly compromise security by clicking phishing links, using weak passwords, or neglecting updates, illustrating the importance of cybersecurity strategies that consider both technical and human factors [6].

However, these technical defense solutions for cyber attacks are not sufficient, as cybersecurity is not solely a technical challenge. Understanding user behavior in cyber-attack situations is critical, as decisions made in real time can determine whether an incident escalates or is quickly contained. However, studying these behaviors presents significant challenges. Cyber-attack scenarios are often unpredictable, and privacy considerations further complicate real-time behavioral analysis. Current methodologies, such as log analyses and static monitoring, provide only limited insights, focusing mainly on retrospective data that may miss the nuances of in-the-moment decision-making during attacks [7]. Additionally, simulation tools used for cybersecurity training tend to lack realistic engagement, which can limit their effectiveness in capturing genuine user responses. A review of the available methods—spanning psychological models, game theory, and simulators—shows that many studies capture only isolated aspects of user behavior, highlighting a need for more comprehensive, multidimensional approaches [8].

Emerging technologies, such as Extended Reality (XR) and Generative AI, hold the potential for developing more comprehensive tools to study user behavior under realistic cyber-attack scenarios. XR technologies, which encompass Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR), offer immersive, interactive environments where user responses and decision-making processes can be observed in real time [9]. Combined with AI-driven simulation capabilities, these technologies can create more accurate models of user behavior, enhancing the development of cybersecurity strategies tailored to human factors. This paper presents a novel framework that integrates digital twin simulations with gamified storytelling through XR and Generative AI, providing a platform to support detailed behavioral studies and improve resilience against cyber attacks.

The framework's unique structure consists of three modules: the Player Behavior Module (PBM), Gamification Module (GM), and Simulation Module (SM), as depicted in Figure 1. These modules work together to deliver a dynamic platform that enables the observation and analysis of user behavior, aiding in the identification of vulnerabilities and the enhancement of response strategies. The modules are further expanded upon in Section 4. We demonstrate the framework's practical application through a case study, where it is implemented within an immersive cybersecurity simulator tailored for a wastewater treatment facility. This simulator allows professionals to engage with simulated cyber-attack scenarios while performing routine monitoring tasks, offering valuable insights into user behavior and decision-making under authentic conditions.

This paper is structured as follows: In Section 2, we present a review of existing studies on user behavior in cybersecurity, covering psychological models, game theory-based approaches, and simulator-based studies and discussing their contributions and limitations. In Section 4, we introduce our proposed XR-based framework, detailing the roles and functionalities of the PBM, GM, and SM. We then present our results from the implementation of this framework in a cybersecurity simulator for wastewater treatment facilities, illustrating its application in a critical infrastructure context, in Section 5. In Section 6, we explore the practical challenges in deploying the framework and its potential applications across other domains. Finally, in Section 7, we conclude with a discussion of the framework's impact on cybersecurity resilience and outline future research directions to further enhance user behavior modeling in high-stakes environments.

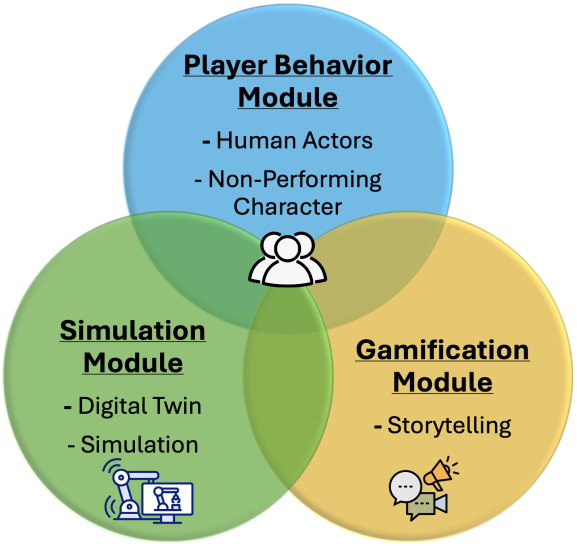


Figure 1. An interaction diagram of the integrated framework depicting the services being offered by each module.

2. Review of User Behavior Studies in Cybersecurity

Understanding user behavior during cyber attacks is crucial for developing effective cybersecurity strategies. Several methodologies have been used in the literature to study user behavior during cybersecurity attacks. These methodologies can broadly be classified into three categories: theoretical modeling-based, game theory-based, and simulator-based approaches, as depicted in Figure 2. Each offers unique insights and tools for analyzing the actions of defenders, attackers, and general network users. By examining these methodologies, we identify gaps in current research and potential opportunities ahead.

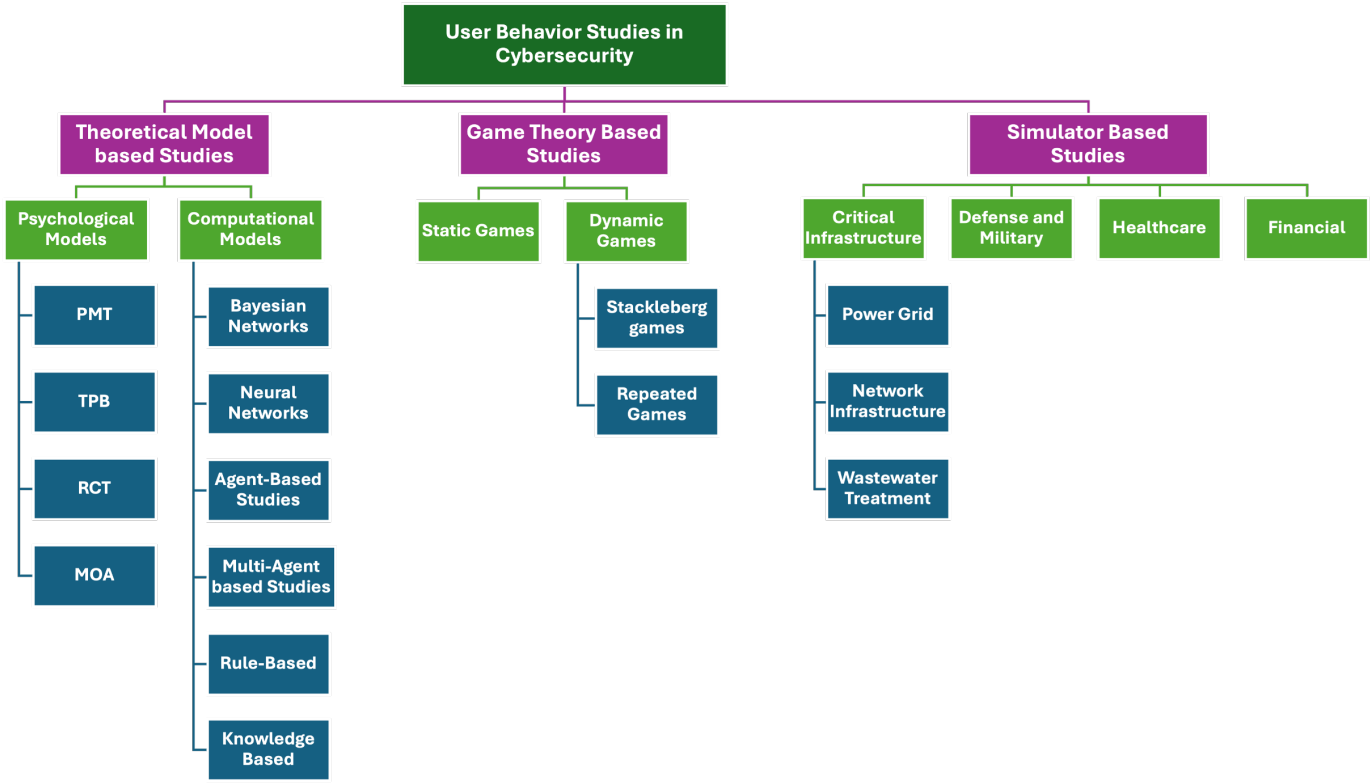


Figure 2. Classification of the various methodologies used in the literature to study user behavior during cybersecurity attacks.

2.1. Theoretical Models

Several theoretical models have been applied to provide insights into the motivations, decision-making processes, and actions of defenders, attackers, and network users during such attacks [10]. These models range from psychological frameworks to advanced computational approaches.

Protection Motivation Theory (PMT) and the Theory of Planned Behavior (TPB) are key psychological models for understanding user behavior in cybersecurity. PMT explains how individuals protect themselves based on perceived threat severity, vulnerability, and self-efficacy. Studies show that higher perceived threat levels lead to stronger protective behaviors, especially against phishing attacks [11–13]. The TPB adds that behavior is influenced by attitudes, norms, and perceived control. Research confirms that these factors impact policy compliance significantly [14,15]. Rational Choice Theory (RCT) and Motivation Opportunity Abilities (MOA) extend this to attackers. They analyze attackers' decisions through cost–benefit evaluations [16]. Studies also suggest that enhancing security and increasing perceived risks deter attacks, reducing the appeal of potential rewards [17–19].

In addition to psychological approaches, computational approaches are increasingly utilized to model and understand user behavior. Bayesian Networks are probabilistic graphical models that are useful for modeling uncertainty and making inferences based on incomplete information. Ref. [20] demonstrated their effectiveness in dynamic risk assessment, intrusion detection, and the evaluation of attack scenarios. Another advanced computational approach involves neural networks, particularly deep learning models, which detect patterns and anomalies in large datasets. Refs. [21,22] developed neural network-based intrusion detection systems and malware detection models, respectively. This illustrates the versatility of neural networks in cybersecurity applications.

In recent times, Agent-Based Systems and Multi-Agent Systems (MASs) [23] have been utilized to model the interactions of autonomous agents. These are effective for simulating complex scenarios. Refs. [24–26] studied malware propagation and defense strategies, demonstrating the potential for realistic simulations of cyber threats and strategic interactions between attackers and defenders. Lastly, Rule-Based Systems [27] and Knowledge-Based Systems [28] have also been used for automated threat analysis, intrusion detection, and network security management. These computational models highlight the role of autonomous agents in enhancing situational awareness and decision-making.

In summary, theoretical models ranging from psychological frameworks to advanced computational models offer valuable insights into user behavior in cybersecurity. These models help predict actions and decisions, providing a basis for developing strategies to enhance security practices, prevent attacks, and mitigate the impact of cyber incidents.

2.2. Game Theory-Based Studies

Game theory, a mathematical framework for analyzing strategic interactions, is widely used to study cybersecurity behavior. Modeling attacker–defender interactions as games enables researchers to predict strategic decisions and possible outcomes. Defenders aim to protect assets, while attackers exploit vulnerabilities, each adapting strategies based on the other's actions. This structured approach provides a strong foundation for understanding cybersecurity behaviors, complementing psychological models with a mathematically grounded analysis of user interactions.

One of the simplest forms of game theory used in cybersecurity is the static game of complete information, where players' strategies and payoffs are common knowledge. Static games of complete information are foundational in game theory applications to cybersecurity, where all players know each other's strategies and payoffs. These games analyze simultaneous interactions without temporal progression, making them ideal for straightforward attack–defense scenarios. For instance, ref. [29] utilized a static game to model intrusion detection systems, where attackers choose to either attack or not, and defenders decide whether to monitor or ignore. Ref. [30] extended this work to cyber-physical

systems, emphasizing optimal defense mechanisms balancing costs and potential damage. Ref. [31] also used game-theoretic approaches to benchmark security risks in cyber-physical systems, demonstrating how static games can aid strategic decision-making.

Building on the static model, dynamic games of incomplete information incorporate the aspect of learning and adaptation over time. Here, players do not have perfect information about others' actions or payoffs. Ref. [32] employed this approach to model network security, considering the evolving strategies of both attackers and defenders. Several other works, like [33–35], use the game-theoretical approach and highlight the importance of adaptive defense mechanisms and the value of deception in cybersecurity.

Moving toward a hierarchical dynamic game structure, Stackelberg games [36] involve a leader–follower dynamic, typically with the defender committing to a strategy first and the attacker responding optimally. Ref. [37] applied the Stackelberg game model to cybersecurity resource allocation, demonstrating how defenders can optimize their strategies by anticipating attacker responses. This model is particularly useful for designing security protocols that are robust against strategic adversaries, as utilized in [8,38,39]. Following the hierarchical approach of Stackelberg games, repeated games capture interactions that occur repeatedly over time, allowing for the analysis of long-term strategies and cooperation possibilities. Ref. [29] explored repeated games in the context of intrusion detection, showing how history and reputation influence strategies. This approach emphasizes the significance of learning and adaptation in ongoing cybersecurity engagements [40,41].

Game-theoretic approaches include static and dynamic (Stackelberg and repeated) games that offer structured frameworks to analyze and predict strategic interactions between attackers and defenders. The results and observations from these studies help researchers develop more robust and adaptive cybersecurity strategies. This not only helps mitigate cyber threats but also helps adapt to the evolving cyber landscape, ultimately enhancing the overall security and resilience against complex cyber adversaries.

2.3. Simulator-Based Studies

The next class of studies is simulator-based studies. These studies offer a distinct and complementary approach to understanding user behavior during cyber attacks compared to game theory-based and psychological models. While game theory focuses on strategic interactions and theoretical models delve into motivational factors, simulators provide a practical and experimental environment where these theories can be applied and tested under controlled conditions [42]. This practical application allows researchers to observe behaviors in real time and under varying conditions, offering empirical evidence that validates or challenges theoretical predictions [43].

Simulator- and modeling-based studies often focus on specific domains, tailoring the simulation environments to reflect the unique challenges and requirements of different sectors. Critical infrastructure sectors, including power grids, water supply systems, and network security, use simulators like PowerWorld [44], EPANET [45], and DETER (Cyber Defense Technology Experimental Research) [46] to model and study the impact of cyber attacks. These tools help in assessing the vulnerabilities and resilience of critical systems, providing insights into how operators manage and mitigate risks during cyber incidents [47]. DETER helps create realistic network environments, where researchers can simulate attacks such as DDoS (distributed denial of service) and evaluate the effectiveness of various defensive strategies. These studies help understand how network administrators and automated systems respond to real-time threats [48].

Military and defense sectors employ sophisticated simulators to model cyber warfare scenarios. These tools enable the study of offensive and defensive strategies in a controlled environment, providing valuable insights into the behavior of military personnel during cyber conflicts [49]. In the healthcare domain, simulators have been used to study the impact of cyber attacks on medical devices and hospital networks. Tools like the Healthcare Cybersecurity Simulation (HCSS) [50] model patient data breaches and ransomware attacks, helping healthcare professionals understand the risks and develop effective response

strategies [51,52]. Similarly, financial institutions also use simulators to model cyber attacks on banking systems and stock exchanges [53]. These simulations help understand the economic impact of cyber incidents and the behavior of financial professionals under stress, guiding the development of robust cybersecurity protocols [54].

Simulator- and modeling-based studies enable a deeper and more empirical understanding of user behavior during cyber attacks. By designing simulations for specific domains, these studies offer targeted insights that help in developing effective, domain-specific cybersecurity strategies. This approach not only validates theoretical models but also bridges the gap between abstract theory and real-world application, enhancing the overall robustness and adaptability of cybersecurity measures.

3. Motivation and Problem Definition

Despite the substantial progress made in understanding user behavior during cyber attacks through theoretical modeling, game theory-based studies, and simulator-based studies, significant challenges remain. One major challenge is the fragmented nature of current research. Most studies tend to focus on one aspect of user behavior, either through psychological modeling, game-theoretic approaches, or simulator-based methods, without integrating these perspectives into a unified framework [8].

Theoretical models offer insights into the motivations and cognitive processes of users, attackers, and defenders, but they often lack the dynamic context that game theory and simulators provide, limiting their ability to predict real-time behavior under cyber threats [11]. Game theory, while useful for analyzing strategic interactions, can oversimplify human behavior, leading to conclusions that miss the complexities of decision-making [29]. Simulator-based studies replicate real-world scenarios, offering a practical, experimental approach, yet may lack the depth of psychological insights and strategic nuances of game theory [43]. Additionally, simulators tend to focus narrowly on domains like network security or critical infrastructure without encompassing the broader psychological and strategic factors impacting behavior across contexts [42,51]. Integrating data and insights from these diverse methodologies is challenging, as each has distinct assumptions, limitations, and data requirements, complicating efforts to build a comprehensive model of user behavior in cybersecurity.

Emerging technologies such as XR and AI offer promising pathways for combining theoretical models, game-theoretic frameworks, and simulator-based approaches, fostering a deeper understanding of user behavior during cyber attacks. XR's immersive environments allow researchers to observe user responses in real time under highly lifelike conditions, capturing nuanced behaviors that may be oversimplified or overlooked in traditional approaches [55]. By creating environments where users interact directly with realistic cyber threats, XR enables the study of decision-making processes and adaptability in scenarios that closely resemble real-world contexts [56].

AI-driven analytics add a powerful dimension to this setup, enabling the processing of large datasets to identify intricate patterns in user behavior, including decision-making tendencies, adaptability, and stress responses. Through machine learning algorithms, AI can uncover insights from behavioral data that inform cybersecurity strategies, providing a tailored approach to both individual and group behaviors [57,58]. This combination of XR and AI thus supports the development of cybersecurity strategies that are responsive to real-time user dynamics, enhancing both the accuracy of user behavior models and the effectiveness of threat detection and response frameworks.

This integrated framework brings together the motivational insights of theoretical models, the strategic interactions captured in game theory, and the empirical realism of simulators within an XR context, allowing for a multidimensional analysis of user behavior. Combining these methodologies provides a more holistic view, helping researchers and practitioners develop adaptive cybersecurity protocols that account for real-world human tendencies and cognitive biases during cyber threats. Implementing such a framework

could lead to more effective threat detection, enhanced resilience strategies, and proactive measures to safeguard against increasingly sophisticated cyber adversaries.

4. Proposed Framework

To address the identified research gaps, we propose a framework to help design and develop a domain-specific system that will guide user behavior studies during cyber attacks. From the review of existing studies on user behavior, we learn that incorporating psychological insights and game-theoretic models into simulations can provide a deeper understanding of user motivations and cognitive biases. This framework integrates three distinct yet complementary modules: the Player Behavior Module (PBM), the Gamification Module (GM), and the Simulator Module (SM), as depicted in Figure 3. Each module leverages insights from psychological modeling, game theory, and simulation studies to provide a holistic approach to understanding user behavior in cybersecurity contexts. Additionally, the incorporation of XR and AI into each module further enhances its capabilities, making the framework more adaptive, intelligent, and effective.

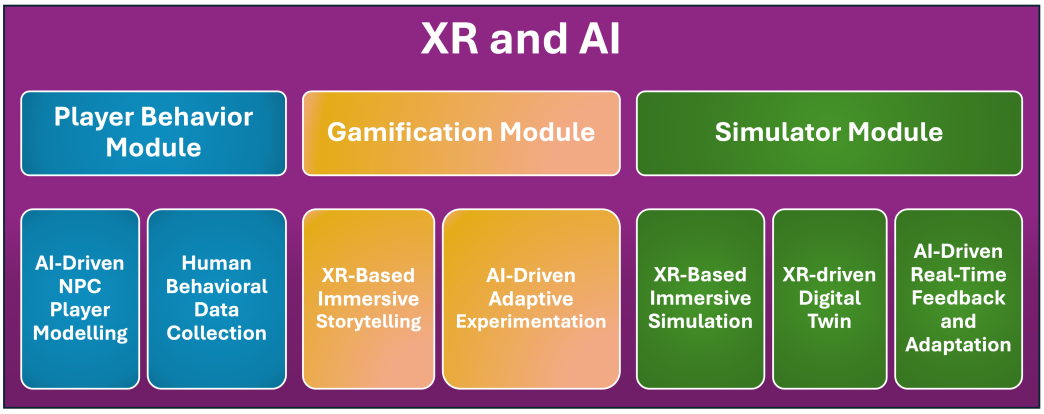


Figure 3. The image depicts the three modules of our proposed framework: Player Behavior Module, Gamification Module, and Simulator Module.

This integrated framework aims to address the multifaceted nature of cybersecurity by integrating insights from various methodological approaches and leveraging advanced technologies. The goal of the developed framework is to holistically understand user behavior. This will help DETECT potential attacks and build robust systems to MITIGATE cyber attacks.

The research methodology for developing this framework involved an extensive literature review and iterative design approach to incorporate and adapt insights from psychology, game theory, and simulation studies. Initially, a review of existing studies on user behavior during cyber attacks was conducted to identify gaps in current methodologies, particularly in capturing realistic and adaptive user responses in high-stress, simulated environments. This foundational review informed the design of three core modules within the framework: PBM, GM, and SM.

To validate the functionality and effectiveness of the proposed framework, we implemented a case study involving a cybersecurity simulator for wastewater treatment facilities. This case study provided a controlled environment to study user behavior under realistic cyber-attack scenarios, allowing for continuous data collection and analysis of user responses, decision-making patterns, and cognitive biases. Observations from this implementation contributed to refining the framework's adaptive features and confirmed its potential for studying user behavior in cybersecurity across various critical domains.

4.1. Player Behavior Module

The Player Behavior Module (PBM) is a foundational element of our proposed framework, dedicated to simulating the actions and interactions of attackers and defenders

within a cyber environment. This module is designed to understand and model player behavior by modeling each user type independently with a predefined set of potential actions they might take within the game environment. These actions are evaluated based on their effectiveness in achieving the overarching objectives of each user type, thereby providing a detailed understanding of motivational factors and decision-making processes.

4.1.1. AI-Driven NPC Player Modeling

The primary objective of the PBM is to model user behavior accurately, drawing upon insights from historical psychological and theoretical models while integrating advanced AI algorithms and LLMs. This framework and module consists of three user types:

1. Attackers: The module models cyber attackers using different tactics, techniques, and procedures that they might employ to breach a system's defenses. This includes activities such as phishing, exploiting vulnerabilities, or launching denial-of-service attacks. By understanding the motivational factors driving attackers, such as financial gain, political motives, or the challenge itself, the PBM can predict potential new attack vectors and evolving strategies.
2. Defenders: These are the users responsible for securing systems against threats, employing strategies like monitoring network activity, patching vulnerabilities, and responding to alerts. The PBM models defender behavior to identify optimal resource allocation strategies, understand the impact of different defense tactics, and predict defender responses to various types of attacks. This predictive capability is crucial for developing proactive defense strategies and improving incident response times.
3. General users: These include non-expert users who interact with systems and unknowingly introduce vulnerabilities, such as through phishing or weak password management. By modeling their behaviors under various simulated attack scenarios, we can better understand how user training and awareness impact overall security.

User behavior during cyber attacks has traditionally been modeled using theories of human behavior, decision-making, and risk perception. While these models are valuable, they often lack the adaptability needed for today's fast-evolving cyber threats. Integrating LLMs significantly enhances these models by using AI algorithms to analyze extensive datasets, identify patterns, and predict future behaviors. LLMs also generate realistic, contextually relevant responses, simulating complex interactions [59]. These insights continuously refine behavioral models, enabling more accurate and nuanced simulations of attacker and defender strategies. The Gamification Module details these player interactions, while the Simulation Module sets the context and environment for them.

4.1.2. Human Behavioral Data Collection and Analysis

Collecting accurate and comprehensive player behavior data is crucial for the effectiveness of the PBM. Various methods can be employed to gather the data, like monitoring network traffic, analyzing system logs, conducting phishing simulations, and employing user surveys [60]. Additionally, honeypots and cyber ranges can be used to observe attacker behavior in a controlled environment [61]. XR technologies also enable the collection of comprehensive interaction data, capturing nuanced user actions and responses in a controlled yet realistic setting. In XR environments, data can be collected on user interactions, decision-making processes, and responses to simulated cyber threats. This includes tracking eye movements, reaction times, and the sequence of actions taken by users [62]. Through these data, researchers can gain valuable insights into their decision-making processes and identify areas for improvement in cybersecurity training.

Integrating AI algorithms and LLMs into data analysis offers considerable benefits. AI can analyze vast datasets to identify patterns and trends in user behavior, improving predictive models [63]. Machine learning techniques, like neural networks, decision trees, and support vector machines, reveal correlations and causations often missed by traditional methods. LLMs add further value by processing data to generate adaptive, real-time responses within the model, keeping simulations relevant to evolving threats and

user strategies [64]. This personalization, based on past user performance, enhances the accuracy and applicability of the PBM, making it a powerful tool for cybersecurity training and research.

In summary, this module is designed to leverage advanced AI algorithms and LLMs for providing a sophisticated and adaptive tool for modeling user behavior in cybersecurity contexts. By integrating comprehensive data collection methods and continuously refining models based on AI-driven insights, the PBM enhances our understanding of attacker, defender, and user actions, contributing to a more robust cybersecurity posture.

4.2. Gamification Module

The Gamification Module is the next crucial component of our proposed framework, leveraging storytelling to create immersive narratives that elucidate various aspects of cybersecurity phenomena or designs. The primary objective of this module is to deeply engage the audience, ensuring that users are not merely passive recipients of information but active participants in the learning process. This engagement is vital because it helps users internalize the lessons and strategies needed to effectively respond to cyber threats.

4.2.1. XR-Based Immersive Storytelling

In the GM, storytelling serves as a tool for crafting engaging, realistic narratives that help users explore complex cybersecurity scenarios firsthand. Here, we focus on developing scenarios where users experience the dynamics, decision-making challenges, and impacts of cyber attacks as though they were happening in real life. These scenarios simulate realistic cybersecurity threats, allowing users to interact with virtual elements that mimic real-world vulnerabilities and attack vectors.

The goal of the scenarios is to provide hands-on interaction, which allows users to identify and respond to subtle cues that are integral to threat detection and risk assessment. Each narrative places users at the center of cyber incidents, requiring them to detect, adapt, strategize, and make crucial decisions based on limited or ambiguous information—skills essential for resilience in actual cybersecurity situations. This helps in honing the critical thinking and decision-making processes necessary for real-world cybersecurity tasks [65].

Moreover, the GM integrates storytelling techniques such as branching storylines and character development to enhance realism and engagement [66]. Branching storylines allow scenarios to unfold differently based on user choices, closely mirroring the unpredictability of real-world cybersecurity [67]. This adaptability makes it possible to capture a wide range of behaviors as users follow various paths to resolution. Character dynamics within the narratives also play a role, with users encountering simulated team members, adversaries, or bystanders, adding a layer of interpersonal decision-making that reflects the collaborative nature of cybersecurity operations [68].

The scenario narratives developed here are implemented within the Simulation Module, where they are brought to life in fully interactive and controlled environments. The SM takes the narratives and storytelling elements created in the GM and integrates them into high-fidelity, immersive XR-based simulations that accurately reflect real-world cybersecurity contexts. By embedding these narratives into the SM, we achieve a seamless transition from narrative design to hands-on simulation, providing users with a cohesive experience that enhances both engagement and behavioral analysis. By merging storytelling with XR technologies, the framework enables immersive, interactive experiences that allow researchers to observe users' responses to cybersecurity challenges in real time [9,66]. The combination of storytelling, advanced XR environments, and tailored scenarios offers a scalable, adaptable framework that supports an in-depth analysis of user behavior across a broad spectrum of cybersecurity situations.

4.2.2. AI-Driven Adaptive Experimentation

The GM also includes an experimentation component, which focuses on the experiments conducted within the developed immersive environments that are tailored to meet

diverse user needs and engagement levels. This is pivotal for designing and conducting interactive experiments that simulate cyber-attack and defense scenarios. These experiments facilitate interactions between the various players in the game. The immersive narrative-based game environment provides a sandbox where behaviors can be observed and analyzed. This has been widely implemented in game-based learning for STEM education [69]. This setup provides valuable insights into how different types of users react to various threats and pressures, highlighting patterns and deviations in behavior. The data collected from these interactions can then be used to refine the models and strategies within the PBM, enhancing the overall effectiveness of the framework. Through this iterative process, the GM contributes to a more nuanced and comprehensive understanding of user behavior in cybersecurity contexts.

LLMs such as GPT-4 can be integrated to generate natural language responses and scenarios, simulating realistic dialogues between users and virtual characters [70]. This level of interaction not only enhances user training but also deepens the understanding of threat dynamics. They can be fine-tuned with cybersecurity-specific datasets to craft accurate and contextually appropriate interactions within the gamified environment. Previous research has underscored the effectiveness of using LLMs to simulate realistic dialogues and scenarios, which are essential for creating accurate and engaging behavioral models [71,72]. Hence, the incorporation of advanced technologies such as LLMs and immersive storytelling into the GM ensures that the simulated environments are not only realistic but also capable of evolving in line with emerging cyber threats and defense strategies.

4.3. Simulator Module (SM)

This module leverages XR technologies and AI to create immersive, interactive simulations of cyber-attack scenarios that closely mimic real-world environments. This module integrates XR's immersive experience with AI-driven behavior modeling to provide a dynamic, adaptive platform for analyzing user responses and defensive strategies. By creating a simulated but realistic environment, the module allows for the comprehensive testing and refinement of cybersecurity strategies in mission-critical systems.

4.3.1. XR-Based Immersive Simulations

At the core of the SM is the ability to provide fully immersive, interactive simulations using VR, AR, and MR. These XR technologies create a lifelike environment in which users engage directly with simulated cyber attacks, allowing for a more realistic experience than traditional 2D interfaces or game-like environments.

- Immersive Cyber-Attack Scenarios: VR environments place users in realistic 3D spaces, such as corporate offices, where they engage with virtual systems under simulated attacks like phishing or ransomware. These immersive scenarios drive real-time decision-making and deepen understanding of cyber threats by situating users within high-stakes, time-sensitive contexts.
- MR in Critical Systems: MR enables scenarios that overlay digital threats onto physical infrastructures like power grids or healthcare systems. With AR glasses, users visualize cyber attacks affecting physical components, offering an authentic view that mirrors real operational environments, which enhances situational awareness and response accuracy.
- Dynamic Scenario Adaptation: The SM's AI-driven adaptability tailors each scenario to the user's expertise, ensuring relevance for both novices and experts. Branching narratives in the GM enable multiple outcomes based on user actions, creating a dynamic training environment that captures genuine behavioral responses to cyber threats [73].

By combining the narrative depth from the GM with the high-fidelity, XR-based simulations in the SM, the framework provides users with a cohesive, interactive experience. This setup not only enhances engagement but also provides researchers with rich data for analyzing user behavior, supporting the development of more effective cybersecurity strategies.

4.3.2. AI-Driven Real-Time Feedback and Adaptation

AI plays a crucial role in enhancing the realism and effectiveness of the SM. By using AI to drive real-time feedback and adaptability, the SM can simulate complex attacker behavior, predict user responses, and adjust the simulation accordingly to provide a more comprehensive analysis of cybersecurity strategies.

- Predictive Analytics for User Behavior: AI can analyze user behavior in real time, predicting how users will react to specific attack vectors based on past interactions and common behavioral patterns. By processing data such as decision-making speed, task completion accuracy, and responses to simulated attacks, AI models can offer predictive insights. For instance, if a user is slow to react to a phishing email in the simulation, AI might predict similar hesitation in future, more critical scenarios, allowing for targeted training interventions.
- Adaptive Training Feedback: The SM uses AI to deliver real-time feedback that adapts to the user's actions. If a user successfully mitigates a simulated attack, AI algorithms adjust the complexity of subsequent scenarios, progressively increasing the difficulty level. Conversely, if a user struggles, the system provides tailored feedback and simpler scenarios to improve skills. This adaptive approach ensures that training remains challenging yet accessible, optimizing learning outcomes.

4.3.3. XR-Driven Digital Twin

A key advancement in the SM is the integration of digital twin technology, powered by XR and AI, to simulate critical infrastructure systems. A digital twin is a virtual representation of a physical system that allows real-time monitoring and interaction.

In this module, digital twins of critical systems (e.g., power grids, healthcare systems, financial networks) are created within an XR environment [74]. Users can interact with these systems using VR or AR interfaces, allowing them to observe and manipulate both the virtual and physical aspects of the system. For example, an XR-based digital twin of a financial network might allow cybersecurity professionals to monitor real-time virtual transactions, identifying suspicious activities while interacting with physical and digital elements [75]. This immersion enables users to gain a holistic understanding of the systems they defend. XR-based digital twins enable users to visualize and mitigate these cascading effects, providing a more comprehensive defense strategy [76].

In conclusion, the proposed framework offers a comprehensive approach to studying user behavior during cyber attacks by integrating insights from psychological modeling, game theory, and simulation studies. By leveraging the unique capabilities of the three modules, PBM, GM, and SM, the framework provides a dynamic, adaptable environment that closely resembles real-world cybersecurity contexts. Through AI-driven data analysis, immersive storytelling, and XR-based simulations, this framework enables a nuanced understanding of attacker, defender, and general user behaviors, capturing the complexity of human decision-making under cyber threats. The integration of XR and AI across all modules enhances realism, responsiveness, and scalability, providing researchers with valuable behavioral insights that can inform the development of more robust cybersecurity strategies. Ultimately, this framework supports a holistic approach to cybersecurity, offering both predictive and preventive insights that strengthen system resilience and preparedness in an ever-evolving threat landscape.

5. Results

Here, in this section, we detail the implementation of the framework in an immersive training simulator developed for wastewater treatment facilities. We also detail our learnings and findings from the full implementation of the system.

5.1. Case Study Implementation of the Framework

This subsection details the implementation of a cybersecurity simulator designed to study user behavior under cyber-attack scenarios, specifically for professionals in wastew-

ater treatment facilities. Using the Oculus Quest 2, the simulator creates an immersive VR environment that integrates the three modules from our framework: Player Behavior Module, Gamification Module, and Simulator Module. Through the dual approach of behavioral analysis and training, this simulator offers operators an environment that reflects both routine tasks and realistic cybersecurity challenges, enabling us to observe, analyze, and enhance user responses to cyber threats.

The primary purpose of this simulator is to capture insights into user behavior, such as decision-making processes, cognitive biases, and response patterns, while equipping operators with the skills to identify and mitigate cyber threats. This case study exemplifies the application of our framework to provide actionable data on how users respond to cyber attacks while reinforcing their cybersecurity awareness in the critical infrastructure context.

5.1.1. System Design Based on the Proposed Framework

The system is developed in line with the three modules of the proposed framework, creating a seamless blend of normal operations and cybersecurity training, as depicted in Figure 4. Our implementation techniques are informed by insights gained from our previous XR-based training simulator projects in cybersecurity [77]. The simulator provides users with a dual experience: they can perform their usual monitoring and maintenance tasks and also be exposed to dynamic cyber-attack scenarios, thus simulating a realistic work environment.

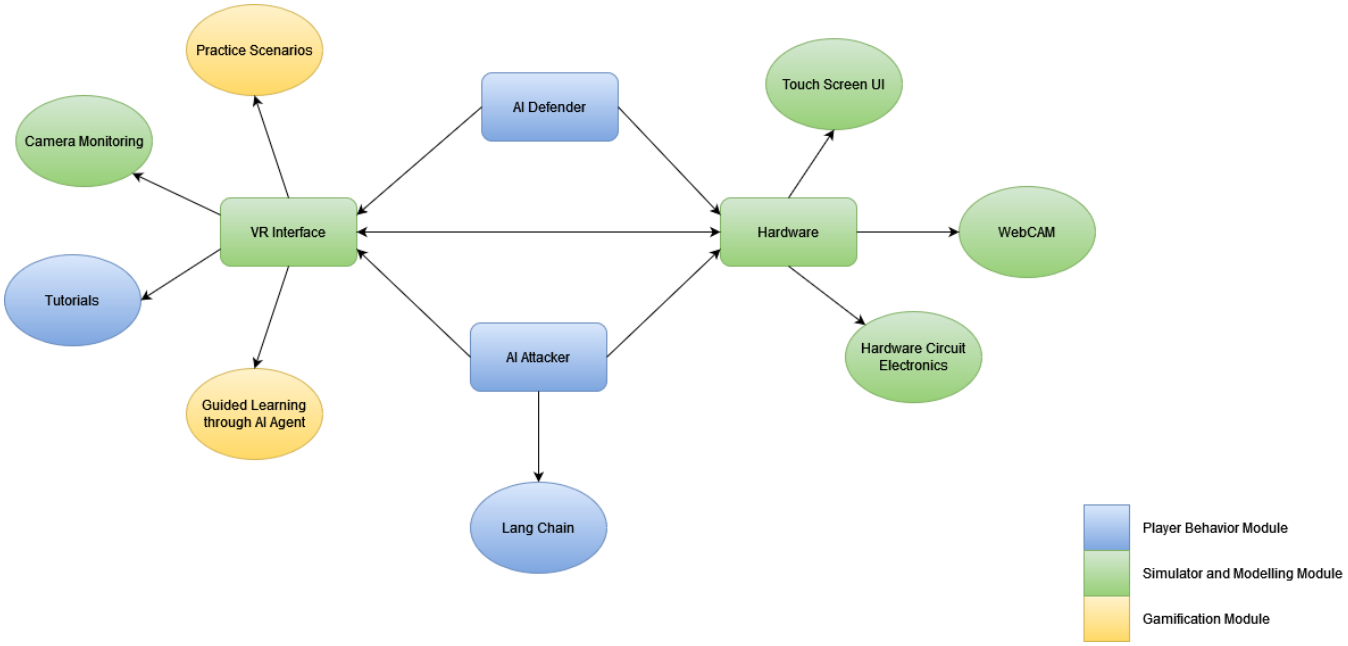


Figure 4. A case study design implementing the proposed framework.

5.1.2. Features Implementing PBM

The PBM focuses on capturing and analyzing operator actions during routine and cyber-attack scenarios. By integrating AI-driven attackers that adjust based on user behavior and a static defender model, the PBM creates an environment that highlights user adaptability and independent decision-making. By tracking metrics like reaction times and accuracy, it provides insights into how operators handle normal and high-stress situations, forming a basis for both training and behavior analysis.

1. AI-Driven Attacker Simulation: AI-driven attackers are able to adapt their tactics based on user actions by utilizing ChatGPT's 4o LLM model within the LangChain framework in a Python Script. In our platform, we focus on generating the following evolving threats: Input Data manipulation and Output Data manipulation, which are both variations of man-in-the-middle attacks and denial-of-service attacks. We

achieve these tasks by using ARPSPOOF, a Python library tool that allows us to perform an Address Resolution Protocol Spoofing attack. This attack allows packets intended for a user to be rerouted into our computer. From there, we can use the Linux operating system's IP forwarding table/rules to either drop packets or perform some type of packet modification. Packet modification is performed with the help of the Scapy packet manipulation library. This allows us to parse Internet packet headers to identify packets of interest and perform modifications at the appropriate spot to prevent any type of data corruption.

2. Static Defender: The static defender setup isolates user responses, enabling a focused study of how operators detect and respond to threats without active system defenses. The ChatGPT 4o model can be used for this with its memory feature, so it can keep track of all of the user's responses to then provide a comprehensive feedback loop back to the operator on how they can improve their response to threats.
3. Behavioral Tracking in Routine and Crisis: Continuous data collection tracks user responses in both normal conditions and crises, measuring reaction times, accuracy, and adaptability under cyber-attack conditions. Again, ChatGPT's memory feature here can be used for the collection and processing of data to provide a result analysis.
4. Tutorials: These provide users with a comprehensive orientation, covering essential background knowledge, theoretical cybersecurity concepts, and simulator interaction techniques. This ensures that users understand the critical context behind cyber threats, familiarizing them with specific interaction mechanics within the simulator. Through this, the users gain the knowledge and skills required to navigate the platform effectively, preparing them to make informed, realistic decisions within the simulation.

5.1.3. Features Implementing GM

The GM enhances engagement by blending routine tasks with cyber-attack simulations in a gamified, narrative-driven environment. Routine and crisis tasks are woven together, allowing operators to experience realistic decision-making under pressure. Real-time feedback and adaptive challenges encourage resilience and skill-building, while gamification provides insights into how users balance operational duties with threat responses.

1. Routine Task Challenges: Operators complete standard tasks like adjusting water levels, inspecting valves, and setting a behavioral baseline for comparison with the crisis response. This is implemented within the VR environment that operators would be in using the raycasting interaction technique.
2. Story-Driven Cyber-Attack Interruptions: Periodic AI-driven cyber attacks—such as denial-of-service or data manipulation attacks—interrupt routine tasks, simulating the urgency of real-world cyber incidents.
3. Adaptive Attacker Interactions: Based on user responses, AI attackers may escalate threats, prompting operators to adjust their strategies, thus revealing user adaptability and situational awareness.
4. Real-Time Feedback and Difficulty Adjustment: AI provides immediate feedback and adapts attack difficulty based on performance, helping users develop resilience through graduated challenges.

5.1.4. Features Implementing SM

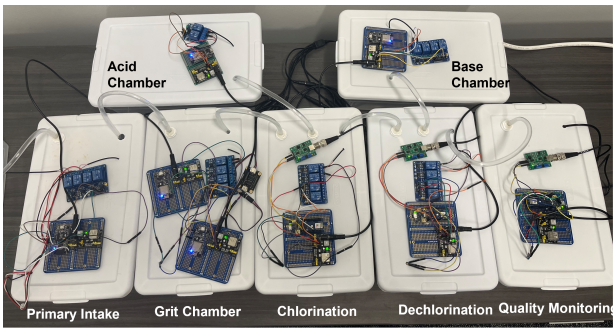
The SM connects virtual actions to a physical testbed, linking VR training to real-world systems. Operators see their actions reflected in a scaled facility through webcam feeds and a digital twin, reinforcing the impact of their decisions. Networked simulations introduce realistic cyber attacks, making the SM a hands-on environment that prepares users for real-life scenarios in critical infrastructure.

1. VR Interface for Realistic Interaction: The VR interface provides a highly immersive view of the facility's layout and equipment, allowing operators to interact with virtual controls and gauges intuitively as depicted in Figure 5. This interface replicates real-world tasks, helping users acclimate to both routine operations and emergency

responses. VR was chosen over MR and AR primarily for its ability to provide a fully immersive experience, which is essential for visualizing the impacts of ongoing cyber attacks within our cybersecurity platform. Simulating these attacks in real life is not feasible due to ethical and safety concerns, but VR allows us to recreate and display these effects in a controlled environment. AR and MR, in contrast, require the user's physical presence at the site to interact with the real-world environment. Additionally, actual wastewater treatment facilities are vast and complex, making it impractical to fully replicate the facility's digital twin interface in AR or MR. However, in scenarios where users are already on-site, AR or MR might be considered, as these technologies can provide context-specific information and interactions within the physical setting. To accomplish this, Unity 2022.3.20f and C# were used to program the various visual effects and interactions possible. Since our VR interface is the virtual component of the digital twin, we need to establish some type of communication link with our hardware to complete the digital twin. We use the Message Queuing Telemetry Transport (MQTT) communication protocol here to ensure that all actions performed on the VR side are mapped/communicated to the physical side. MQTT is a lightweight messaging protocol that consists of a topic and a message. The topic consists of a unique string value, where all messages using that string value communicate on the same channel [78]. We enhance the VR environment with a conversational AI NPC, enabling users to naturally interact with the AI and use it as a learning tool for clarifying various concepts. To accomplish this, we use a Unity asset called Convai (Version 3.2.0), which allows seamless integration with any existing VR environment. Users can easily add an NPC character to the VR setting and customize it to narrate stories or perform specific actions, thanks to the asset's Narrative Design Feature for creating sequential storytelling. The asset leverages GPT-4o as its language model and can store multiple documents to build a knowledge base, enriching contextual interactions.

2. Miniature Testbed Integration: The operators' actions in VR, like adjusting water flow, are mirrored in real time on a physical testbed, demonstrating the real-world impact of decisions. The physical testbed is made up of Arduino components, such as the NodeMCU ESP8266 and Arduino MKR Wifi 1010 microcontrollers. Attached to these microcontrollers are various sensors and motors that are appropriate for the given stage that the hardware represents. These can include water pump(s) to move water from one stage to the other, water level, water temperature, and pH sensors.
3. Webcam Monitoring for Real-Time Impact Observation: Users can monitor physical testbed responses to their virtual actions, emphasizing real-world consequences and situational awareness. This is accomplished by connecting multiple USB webcams to the computer hosting/running the VR application and using Unity's built-in webcam library to retrieve the appropriate webcam feeds.
4. Digital Twin for Enhanced Visualization: A synchronized digital twin displays real-time system conditions, allowing users to observe the effects of cyber attacks and operational adjustments. This is carried out through our Unity VR program, which provides visualizations such as water level movement and water color changes.
5. Simulated Network Components with MQTT: The digital twin's network uses MQTT protocols, enabling AI-driven attacks like denial of service, which allows observation of user responses to network-based threats.

Together, these features create a seamless, integrated platform. They combine adaptive threat simulation, real-time data collection, immersive VR interaction, and physical–virtual synchronization. Aligned with the PBM, GM, and SM, this platform strengthens detection, training, and mitigation capabilities in cybersecurity.



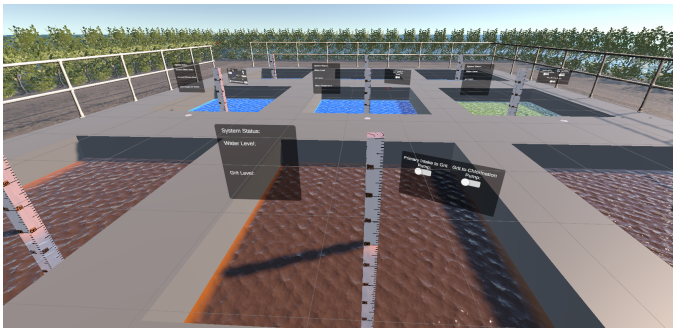


Figure 5. (**Top**) An aerial view of a water treatment facility in Wisconsin [79]. (**Bottom Left**) The hardware of the developed digital twin wastewater treatment facility. (**Bottom Right**) The VR interface of the developed digital twin wastewater treatment facility.

6. Discussion

This section explores the practical challenges and broader applicability of our proposed framework in cybersecurity training and research. Integrating technologies like XR, AI, and digital twins brings both technical and logistical complexities, particularly in high-stakes environments like critical infrastructure. Additionally, we examine the potential for adapting this framework across various domains, where understanding user behavior in response to cyber threats can drive improved security and response strategies.

6.1. Application of the Framework in Other Domains

Understanding user behavior during cyber attacks is pivotal across high-stakes industries where human responses can critically impact the effectiveness of cybersecurity measures. Cyber attacks increasingly target sectors with complex operational demands, such as healthcare [80], finance [81], defense, and utilities, where the consequences of a security breach can be profound, affecting public safety, financial stability, and national security. In these domains, the ability to analyze and anticipate user behavior under simulated attack conditions offers insights that traditional technical defenses alone cannot provide [82].

Our framework, designed to model realistic cyber threats within an immersive gamified XR and digital twin environment, is uniquely suited for these applications. By capturing detailed behavioral responses—such as decision-making processes, reaction times, and adaptability to evolving threats—this framework enables each sector to deepen its understanding of user actions and potential vulnerabilities. By tailoring the framework to address specific environmental challenges and threat types, each domain can gain actionable insights that inform training programs, shape security protocols, and enhance response strategies. Here, we discuss how this framework could be adapted to meet the cybersecurity needs of healthcare, financial services, defense, and utilities. Through domain-specific

simulations, this approach empowers organizations to not only train their personnel but also design security strategies that are resilient to human factors.

1. Healthcare Sector: In healthcare, cyber attacks can compromise not only data integrity but also patient safety [83]. Adapting the framework to simulate attacks on Electronic Health Records (EHRs) or medical devices allows healthcare professionals to experience and respond to realistic cyber threats that could impact patient outcomes [84]. The proposed framework helps collect healthcare-specific behavioral responses, such as how clinicians prioritize between clinical care and cyber threat management or how they recognize and mitigate threats within sensitive healthcare environments. Insights into these behaviors can inform the development of training programs that emphasize both patient safety and security awareness while identifying areas where procedural adjustments or additional safeguards may be required [85].
2. Financial Services: For financial institutions, the complexity of cyber threats often targets not just data security but also operational continuity and customer trust [86]. Using the framework to model scenarios like insider threats, data breaches, and phishing attacks allows finance professionals to engage with simulations that reflect real-world conditions. Behavioral data on decision-making processes, risk tolerance, and speed of response in these environments provide insights that financial institutions can use to strengthen specific areas of their cybersecurity protocols [87,88]. Additionally, the framework can reveal the impact of cognitive biases under stress, helping institutions refine training to mitigate human error in high-stakes financial transactions.
3. Defense and Military Applications: Cybersecurity in defense settings requires readiness for complex, multi-layered threats that could affect national security [89,90]. By simulating hybrid cyber-physical threats on military networks and operational systems [91], this framework can be adapted to study how personnel respond to diverse cyber warfare tactics, such as disruption of communication channels or interference with autonomous systems. Behavioral insights derived from these scenarios—such as response coordination, situational awareness, and the ability to adapt to rapidly evolving threats—are critical for refining defense protocols and designing adaptive training programs that enhance resilience in cyber warfare [92].

The framework's potential to reveal behavioral insights across these domains underscores its versatility and importance. By adapting simulations to meet each sector's unique challenges, this approach provides a comprehensive understanding of user responses to cyber threats, which is essential for developing informed, behavior-centric security practices across critical industries.

6.2. Practical Challenges to Integrating XR, AI, and Digital Twin

Deploying a cybersecurity training system that integrates XR, AI, and digital twin technologies faces multiple technical and logistical challenges, particularly when applied within critical infrastructure environments. The first significant obstacle arises from the integration of AI-driven cyber-attack simulations, especially through LLMs. LLMs like GPT-4o are constrained by safety restrictions that prevent their direct use for simulating certain attack scenarios. While indirect workarounds exist to bypass these limitations, their use can lead to unintended, unpredictable outputs. An alternative solution is to use offline LLMs that have their censorship capabilities removed. However, these offline models are often limited by smaller, less diverse datasets, resulting in decreased performance accuracy and consistency. And, if a larger dataset is desired for offline models, a commercial-grade computer would be needed to host it on. On top of that, companies have policies regarding the use of LLMs due to safety, privacy, and ethical concerns [93]. So, the adoption of this system in corporate training may not be feasible or would take longer. This challenge in balancing ethical restrictions with operational needs requires careful consideration when selecting LLMs for real-time behavior modeling and adaptive threat simulation.

The broader adoption of VR technologies for educational and data collection purposes is another hurdle, as VR remains a relatively emergent field. Despite XR's immersive

advantages, accessibility issues remain, with factors like VR motion sickness, control familiarity, and interface complexity potentially inhibiting widespread user adoption [94]. Although this training system incorporates an initial orientation phase to familiarize users with both VR controls and cybersecurity concepts, there remains a risk of VR-induced discomfort, which can impact user engagement and data quality over longer sessions. Technical adaptability in designing VR controls to be more intuitive, coupled with gradual exposure to VR environments, can help mitigate these effects but may extend training durations and require additional development resources [95].

The deployment of digital twins within specific critical infrastructure environments, such as wastewater treatment facilities, presents additional complexities. Each facility varies considerably in its processing stages, underlying technology stack, and physical layout, requiring extensive customization of the digital twin and VR environment for each installation. This customization demands a tailored virtual design that accurately mirrors the plant's unique physical space, increasing the initial setup cost and requiring specialized development for accurate system replication. Additionally, replicating hardware components to create a cohesive cyber-physical system is a critical challenge. Alternatives like NodeMCU and Arduino microcontrollers provide lower-cost options for creating digital twin setups, but they demand computer engineering expertise for efficient configuration and troubleshooting. These limitations highlight the need for standardized, cost-effective solutions that can ensure reliable XR integration within industrial infrastructures [95].

Overall, addressing these challenges is essential for developing a scalable and effective training system that leverages XR, AI, and digital twin technologies. By refining both the hardware and software aspects, including AI capabilities and VR environment customization, this system holds the potential to advance cybersecurity training in critical infrastructure sectors, creating a more adaptable and resilient approach to security preparedness.

7. Conclusions

In this paper, we propose a framework for studying user behavior during cyber attacks in critical infrastructure. The framework combines psychological modeling, game theory, and immersive simulation through three core modules: the Player Behavior Module (PBM), Gamification Module (GM), and Simulation Module (SM). Together, these modules create a system that captures user responses, decision-making, and adaptability in real time. In this research work, we also successfully implement the framework in a cybersecurity simulator designed for wastewater treatment facilities. This simulator allows operators to practice daily tasks while facing realistic, adaptive cyber threats, offering a controlled space to observe user behavior during attacks. It also builds key skills for threat detection and response, making the training practical for high-stakes environments. Serving as both a tool for behavioral study and training, the simulator shows strong potential to bridge research and real-world applications.

The impact of this work extends beyond research applications, offering valuable tools for developing adaptive and resilient cybersecurity training solutions across critical infrastructure sectors. By providing a simulated environment that closely mirrors real-world conditions, the platform enables operators to develop essential cybersecurity skills, improving their awareness and decision-making abilities in high-stress scenarios. Additionally, this framework supports organizations in understanding how human behavior influences cybersecurity resilience, informing the development of policies and protocols that account for cognitive and behavioral factors.

Future work will include conducting a user study on the platform to gather data on user responses and adaptation in cyber-attack scenarios. This study will focus on understanding decision-making processes, cognitive load, and stress responses during attacks, addressing the current gap in empirical validation. Additionally, the defender model will be gradually adapted to become more robust, allowing us to observe the interplay between attackers, defenders, and users. These insights will contribute to a better

understanding of the dynamics of cybersecurity interactions, supporting the creation of adaptable training protocols that enhance operator resilience in high-risk environments.

Author Contributions: N.D.C. was responsible for methodology development, investigation, and data curation, with a primary focus on the literature review and framework development. She also managed the original draft preparation, synthesizing key findings and structuring the initial manuscript. A.L. led the software development of the XR-based digital twin simulator presented in the results. He contributed to the writing through review and editing, ensuring technical accuracy and clarity in the manuscript. M.A. and D.G. served as faculty advisors, contributing to the conceptualization, methodology, and validation of the research framework. They were actively involved in the review and editing process and secured funding to support the project. All authors have read and agreed to the published version of the manuscript.

Funding: This project is partially sponsored by the Commonwealth Cyber Initiative, an investment in the advancement of cyber R&D, innovation, and workforce development, under the VMIRL Contract No 24-15 CCI SWVA grant. The project is also partially sponsored by the National Security Agency under Grant/Cooperative Agreement Number H98230-21-l-0167.

Institutional Review Board Statement: Not Applicable.

Informed Consent Statement: Not Applicable.

Data Availability Statement: Data are contained within the article.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

The following abbreviations are used in this manuscript:

XR	Extended Reality
AR	Augmented Reality
VR	Virtual Reality
MR	Mixed Reality
AI	Artificial Intelligence
PBM	Player Behavior Module
GM	Gamification Module
SM	Simulator Module
PMT	Protection Motivation Theory
TPB	Theory of Planned Behavior
RCT	Rational Choice Theory
MOA	Motivation Opportunity Abilities
MQTT	Message Queuing Telemetry Transport
SCP	Situational Crime Prevention
LLM	Large Language Models

References

1. Guo, S.; Zeng, D. *Cyber-Physical Systems: Architecture, Security and Application*; Springer: Cham, Switzerland, 2019.
2. Armbrust, M.; Fox, A.; Griffith, R.; Joseph, A.D.; Katz, R.; Konwinski, A.; Lee, G.; Patterson, D.; Rabkin, A.; Stoica, I.; et al. A view of cloud computing. *Commun. ACM* **2010**, *53*, 50–58. [CrossRef]
3. Ghernouti-Hélie, S. A national strategy for an effective cybersecurity approach and culture. In Proceedings of the 2010 International Conference on Availability, Reliability and Security, Krakow, Poland, 15–18 February 2010; pp. 370–373.
4. Han, S.; Xie, M.; Chen, H.H.; Ling, Y. Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE Syst. J.* **2014**, *8*, 1052–1062.
5. Tounsi, W.; Rais, H. A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Comput. Secur.* **2018**, *72*, 212–233. [CrossRef]
6. Sasse, M.A.; Brostoff, S.; Weirich, D. Transforming the 'weakest link'—A human/computer interaction approach to usable and effective security. *BT Technol. J.* **2001**, *19*, 122–131. [CrossRef]
7. Young, H.; van Vliet, T.; van de Ven, J.; Jol, S.; Broekman, C. Understanding human factors in cyber security as a dynamic system. In Proceedings of the Advances in Human Factors in Cybersecurity, Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, Los Angeles, CA, USA, 17–21 July 2017; pp. 244–254.

8. Pawlick, J.; Colbert, E.; Zhu, Q. A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Comput. Surv. (CSUR)* **2019**, *52*, 82. [CrossRef]
9. Alnajim, A.M.; Habib, S.; Islam, M.; AlRawashdeh, H.S.; Wasim, M. Exploring cybersecurity education and training techniques: A comprehensive review of traditional, virtual reality, and augmented reality approaches. *Symmetry* **2023**, *15*, 2175. [CrossRef]
10. Goerger, S.R.; McGinnis, M.L.; Darken, R.P. A validation methodology for human behavior representation models. *J. Def. Model. Simul.* **2005**, *2*, 39–51. [CrossRef]
11. Anderson, C.L.; Agarwal, R. Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions. *MIS Q.* **2010**, 34, 613–643. [CrossRef]
12. Pahnila, S.; Siponen, M.; Mahmood, A. Employees' behavior towards IS security policy compliance. In Proceedings of the 2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07), Big Island, HI, USA, 3–6 January 2007; p. 156b.
13. Boss, S.R.; Galletta, D.F.; Lowry, P.B.; Moody, G.D.; Polak, P. What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Q.* **2015**, *39*, 837–864. [CrossRef]
14. Sommestad, T.; Karlzén, H.; Hallberg, J. The theory of planned behavior and information security policy compliance. *J. Comput. Inf. Syst.* **2017**, *59*, 344–353. [CrossRef]
15. Ifinedo, P. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Comput. Secur.* **2012**, *31*, 83–95. [CrossRef]
16. Ölander, F.; Thøgersen, J. Understanding of consumer behaviour as a prerequisite for environmental protection. *J. Consum. Policy* **1995**, *18*, 345–385. [CrossRef]
17. Runions, K.C.; Bak, M. Online moral disengagement, cyberbullying, and cyber-aggression. *Cyberpsychology Behav. Soc. Netw.* **2015**, *18*, 400–405. [CrossRef]
18. Hirschi, T. On the compatibility of rational choice and social control theories of crime. In *The Reasoning Criminal*; Routledge: Abingdon-on-Thames, UK, 2017; pp. 105–118.
19. Bossler, A. Contributions of criminological theory to the understanding of cybercrime offending and victimization. In *The Human Factor of Cybercrime*; Routledge: Abingdon-on-Thames, UK, 2019; pp. 29–59.
20. Poolsappasit, N.; Dewri, R.; Ray, I. Dynamic security risk management using bayesian attack graphs. *IEEE Trans. Dependable Secur. Comput.* **2011**, *9*, 61–74. [CrossRef]
21. Yin, C.; Zhu, Y.; Fei, J.; He, X. A deep learning approach for intrusion detection using recurrent neural networks. *IEEE Access* **2017**, *5*, 21954–21961. [CrossRef]
22. Alsharafi, L.; Asiri, M.; Azzony, S.; Alqahtani, A. Malware Detection Based on Deep Learning. In Proceedings of the 2023 3rd International Conference on Computing and Information Technology (ICCIT), Tabuk, Saudi Arabia, 10–11 May2023; pp. 427–432.
23. Wooldridge, M. *An Introduction to Multiagent Systems*; John Wiley & Sons: Hoboken, NJ, USA, 2009.
24. Zhang, D.; Feng, G.; Shi, Y.; Srinivasan, D. Physical safety and cyber security analysis of multi-agent systems: A survey of recent advances. *IEEE/CAA J. Autom. Sin.* **2021**, *8*, 319–333. [CrossRef]
25. Belaoued, M.; Derhab, A.; Mazouzi, S.; Khan, F.A. MACoMal: A multi-agent based collaborative mechanism for anti-malware assistance. *IEEE Access* **2020**, *8*, 14329–14343. [CrossRef]
26. Kotenko, I. Multi-agent modelling and simulation of cyber-attacks and cyber-defense for homeland security. In Proceedings of the 2007 4th IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications, Dortmund, Germany, 6–8 September 2007; pp. 614–619.
27. Sarker, I.H.; Kayes, A. ABC-RuleMiner: User behavioral rule-based machine learning method for context-aware intelligent services. *J. Netw. Comput. Appl.* **2020**, *168*, 102762. [CrossRef]
28. Phillips, S.C.; Taylor, S.; Boniface, M.; Modafferi, S.; Surridge, M. Automated knowledge-based cybersecurity risk assessment of cyber-physical systems. *IEEE Access* **2024**, *12*, 82482–82505. [CrossRef]
29. Manshaei, M.H.; Zhu, Q.; Alpcan, T.; Bacşar, T.; Hubaux, J.P. Game theory meets network security and privacy. *ACM Comput. Surv. (CSUR)* **2013**, *45*, 25. [CrossRef]
30. Tushar, W.; Yuen, C.; Saha, T.K.; Nizami, S.; Alam, M.R.; Smith, D.B.; Poor, H.V. A survey of cyber-physical systems from a game-theoretic perspective. *IEEE Access* **2023**, *11*, 9799–9834. [CrossRef]
31. Amin, S.; Schwartz, G.A.; Hussain, A. In quest of benchmarking security risks to cyber-physical systems. *IEEE Netw.* **2013**, *27*, 19–24. [CrossRef]
32. Lye, K.W.; Wing, J.M. Game strategies in network security. *Int. J. Inf. Secur.* **2005**, *4*, 71–86. [CrossRef]
33. Panaousis, E.; Fielder, A.; Malacaria, P.; Hankin, C.; Smeraldi, F. Cybersecurity games and investments: A decision support approach. In Proceedings of the Decision and Game Theory for Security: 5th International Conference, GameSec 2014, Los Angeles, CA, USA, 6–7 November 2014; Proceedings 5; Springer: Berlin/Heidelberg, Germany, 2014; pp. 266–286.
34. Fielder, A.; Panaousis, E.; Malacaria, P.; Hankin, C.; Smeraldi, F. Decision support approaches for cyber security investment. *Decis. Support Syst.* **2016**, *86*, 13–23. [CrossRef]
35. Musman, S.; Turner, A. A game theoretic approach to cyber security risk management. *J. Def. Model. Simul.* **2018**, *15*, 127–146. [CrossRef]
36. Simaan, M.; Cruz, J.B., Jr. On the Stackelberg strategy in nonzero-sum games. *J. Optim. Theory Appl.* **1973**, *11*, 533–555. [CrossRef]

37. Zhu, Q.; Başar, T. Game-theoretic approach to feedback-driven multi-stage moving target defense. In Proceedings of the International Conference on Decision and Game Theory for Security, Fort Worth, TX, USA, 11–12 November 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 246–263.
38. Zhang, Y.; Malacaria, P. Bayesian Stackelberg games for cyber-security decision support. *Decis. Support Syst.* **2021**, *148*, 113599. [CrossRef]
39. Jakóbik, A.; Palmieri, F.; Kołodziej, J. Stackelberg games for modeling defense scenarios against cloud security threats. *J. Netw. Comput. Appl.* **2018**, *110*, 99–107. [CrossRef]
40. Veksler, V.D.; Buchler, N.; LaFleur, C.G.; Yu, M.S.; Lebiere, C.; Gonzalez, C. Cognitive models in cybersecurity: Learning from expert analysts and predicting attacker behavior. *Front. Psychol.* **2020**, *11*, 1049. [CrossRef]
41. Do, C.T.; Tran, N.H.; Hong, C.; Kamhoua, C.A.; Kwiat, K.A.; Blasch, E.; Ren, S.; Pissinou, N.; Iyengar, S.S. Game theory for cyber security and privacy. *ACM Comput. Surv. (CSUR)* **2017**, *50*, 30. [CrossRef]
42. Benzel, T.; Braden, R.; Kim, D.; Neuman, C.; Joseph, A.; Sklower, K.; Ostrenga, R.; Schwab, S. Experience with deter: A testbed for security research. In Proceedings of the 2nd International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, TRIDENTCOM 2006, Barcelona, Spain, 1–3 March 2006; p. 10.
43. Ashok, A.; Govindarasu, M.; Wang, J. Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid. *Proc. IEEE* **2017**, *105*, 1389–1407. [CrossRef]
44. Zhang, D.; Li, S.; Zeng, P.; Zang, C. Optimal microgrid control and power-flow study with different bidding policies by using powerworld simulator. *IEEE Trans. Sustain. Energy* **2013**, *5*, 282–292. [CrossRef]
45. Patriarca, R.; Simone, F.; Di Gravio, G. Modelling cyber resilience in a water treatment and distribution system. *Reliab. Eng. Syst. Saf.* **2022**, *226*, 108653. [CrossRef]
46. Benzel, T. The science of cyber security experimentation: The DETER project. In Proceedings of the 27th Annual Computer Security Applications Conference, Orlando, FL, USA, 5–9 December 2011; pp. 137–148.
47. Le, T.D.; Anwar, A.; Loke, S.W.; Beuran, R.; Tan, Y. Gridattacksim: A cyber attack simulation framework for smart grids. *Electronics* **2020**, *9*, 1218. [CrossRef]
48. Kaur, D.; Sachdeva, M.; Kumar, K. Study of DDoS attacks using DETER Testbed. *Int. J. Comput. Bus. Res.* **2012**, *3*, 1–13.
49. Kostyuk, N.; Zhukov, Y.M. Invisible digital front: Can cyber attacks shape battlefield events? *J. Confl. Resolut.* **2019**, *63*, 317–347. [CrossRef]
50. Willing, M.; Dresen, C.; Gerlitz, E.; Haering, M.; Smith, M.; Binnewies, C.; Guess, T.; Haverkamp, U.; Schinzel, S. Behavioral responses to a cyber attack in a hospital environment. *Sci. Rep.* **2021**, *11*, 19352. [CrossRef] [PubMed]
51. Priyadarshini, I.; Kumar, R.; Tuan, L.M.; Son, L.H.; Long, H.V.; Sharma, R.; Rai, S. A new enhanced cyber security framework for medical cyber physical systems. *SICS Softw.-Intensive-Cyber-Phys. Syst.* **2021**,*35*, 159–183. [CrossRef]
52. Butpheng, C.; Yeh, K.H.; Xiong, H. Security and privacy in IoT-cloud-based e-health systems—A comprehensive review. *Symmetry* **2020**, *12*, 1191. [CrossRef]
53. Najaf, K.; Mostafiz, M.I.; Najaf, R. Fintech firms and banks sustainability: Why cybersecurity risk matters? *Int. J. Financ. Eng.* **2021**, *8*, 2150019. [CrossRef]
54. Gomber, P.; Kauffman, R.J.; Parker, C.; Weber, B.W. On the fintech revolution: Interpreting the forces of innovation, disruption, and transformation in financial services. *J. Manag. Inf. Syst.* **2018**, *35*, 220–265. [CrossRef]
55. Chuah, S.H.W. Wearable XR-technology: Literature review, conceptual framework and future research directions *Int. J. Technol. Mark.* **2018**, *13*, 205–259. [CrossRef]
56. Chandrashekar, N.D.; King, K.; Gračanin, D.; Azab, M. Design & development of virtual reality empowered cyber-security training testbed for IoT systems. In Proceedings of the 2023 3rd Intelligent Cybersecurity Conference (ICSC), San Antonio, TX, USA, 23–25 October 2023; pp. 86–94.
57. Ahsan, M.; Nygard, K.E.; Gomes, R.; Chowdhury, M.M.; Rifat, N.; Connolly, J.F. Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *J. Cybersecur. Priv.* **2022**, *2*, 527–555. [CrossRef]
58. Addae, J.H.; Sun, X.; Towey, D.; Radenkovic, M. Exploring user behavioral data for adaptive cybersecurity. *User Model. User-Adapt. Interact.* **2019**, *29*, 701–750. [CrossRef]
59. Sekulić, I.; Terragni, S.; Guimarães, V.; Khau, N.; Guedes, B.; Filipavicius, M.; Manso, A.F.; Mathis, R. Reliable LLM-based user simulator for task-oriented dialogue systems. *arXiv* **2024**, arXiv:2402.13374.
60. Jin, L.; Chen, Y.; Wang, T.; Hui, P.; Vasilakos, A.V. Understanding user behavior in online social networks: A survey. *IEEE Commun. Mag.* **2013**, *51*, 144–150.
61. Dowling, S.; Schukat, M.; Melvin, H. A ZigBee honeypot to assess IoT cyberattack behaviour. In Proceedings of the 2017 28th Irish Signals and Systems Conference (ISSC), Killarney, Ireland, 20–21 June 2017; pp. 1–6.
62. Abraham, M.; Saeghe, P.; Mcgill, M.; Khamis, M. Implications of xr on privacy, security and behaviour: Insights from experts. In Proceedings of the Nordic Human-Computer Interaction Conference, Aarhus, Denmark, 8–12 October 2022; pp. 1–12.
63. Rokhsaritalemi, S.; Sadeghi-Niaraki, A.; Choi, S.M. Exploring emotion analysis using artificial intelligence, geospatial information systems, and extended reality for urban services. *IEEE Access* **2023**, *11*, 92478–92495. [CrossRef]
64. Marín-Vega, H.; Alor-Hernández, G.; Bustos-López, M.; López-Martínez, I.; Hernández-Chaparro, N.L. Extended Reality (XR) Engines for Developing Gamified Apps and Serious Games: A Scoping Review. *Future Internet* **2023**, *15*, 379. [CrossRef]

65. Katual, D.; Drevin, L.; Goede, R. Game-Based Learning to Improve Critical Thinking and Knowledge Sharing: Literature Review. *J. Int. Soc. Syst. Sci.* **2023**, *67*.
66. Naul, E.; Liu, M. Why story matters: A review of narrative in serious games. *J. Educ. Comput. Res.* **2020**, *58*, 687–707. [CrossRef]
67. Gordon, A.; van Lent, M.; Van Velsen, M.; Carpenter, P.; Jhala, A. Branching storylines in virtual reality environments for leadership development. In Proceedings of the National Conference on Artificial Intelligence, Orlando, FL, USA, 18–22 July 1999; AAAI Press: Menlo Park, CA, USA; MIT Press: Cambridge, MA, USA, 2004; pp. 844–851.
68. Gedris, K.; Bowman, K.; Neupane, A.; Hughes, A.; Bonsignore, E.; West, R.; Balzotti, J.; Hansen, D. Simulating municipal cybersecurity incidents: Recommendations from expert interviews. In Proceedings of the Annual Hawaii International Conference on System Sciences, Kauai, HI, USA, 5 January 2021.
69. Lester, J.C.; Rowe, J.P.; Mott, B.W. Narrative-centered learning environments: A story-centric approach to educational games. In *Emerging Technologies for the Classroom: A Learning Sciences Perspective*; Springer: Berlin/Heidelberg, Germany, 2012; pp. 223–237.
70. Wan, H.; Zhang, J.; Suria, A.A.; Yao, B.; Wang, D.; Coady, Y.; Prpa, M. Building LLM-based AI Agents in Social Virtual Reality. In Proceedings of the Extended Abstracts of the CHI Conference on Human Factors in Computing Systems, Honolulu, HI, USA, 11–16 May 2024; pp. 1–7.
71. Radford, A.; Wu, J.; Child, R.; Luan, D.; Amodei, D.; Sutskever, I. Language models are unsupervised multitask learners. *OpenAI Blog* **2019**, *1*, 9.
72. Brown, T.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.D.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; et al. Language models are few-shot learners. *Adv. Neural Inf. Process. Syst.* **2020**, *33*, 1877–1901.
73. Stanney, K.M.; Archer, J.; Skinner, A.; Horner, C.; Hughes, C.; Brawand, N.P.; Martin, E.; Sanchez, S.; Moralez, L.; Fidopiastis, C.M.; et al. Performance gains from adaptive eXtended Reality training fueled by artificial intelligence. *J. Def. Model. Simul.* **2022**, *19*, 195–218. [CrossRef]
74. Chandrashekar, N.D.; Safford, S.; Muniyandi, M.; Gračanin, D. An extended reality simulator for pulse palpation training. In Proceedings of the 2023 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW), Shanghai, China, 25–29 March 2023; pp. 178–182.
75. Barykin, S.; Kapustina, I.; Sergeev, S.; Kalinina, O.; Vilken, V.; De la Poza, E.; Putikhin, Y.; Volkova, L. Developing the physical distribution digital twin model within the trade network. *Acad. Strateg. Manag. J.* **2021**, *20*, 1–24.
76. Rudnicka, Z.; Proniewska, K.; Perkins, M.; Pregowska, A. Cardiac Healthcare Digital Twins Supported by Artificial Intelligence-Based Algorithms and Extended Reality—A Systematic Review. *Electronics* **2024**, *13*, 866. [CrossRef]
77. Lee, A.; King, K.; Gračanin, D.; Azab, M. Experiential Learning Through Immersive XR: Cybersecurity Education for Critical Infrastructures. In Proceedings of the International Conference on Human-Computer Interaction, Washington DC, USA, 29 June–4 July 2024; Springer: Berlin/Heidelberg, Germany 2024; pp. 56–69.
78. MQTT Version 5.0. Edited by Andrew Banks, Ed Briggs, Ken Borgendale, and Rahul Gupta. 7 March 2019. OASIS Standard. Available online: https://docs.oasis-open.org/mqtt/mqtt/v5.0/os/mqtt-v5.0-os.html (accessed on 12 October 2024)
79. Commons, W. La Crosse Wastewater Treatment Facility. 2024. Available online: https://commons.wikimedia.org/w/index.php?curid=150028072 (accessed on 12 October 2024)
80. Lehto, M. Cyber-attacks against critical infrastructure. In *Cyber Security: Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2022; pp. 3–42.
81. Pomerleau, P.L.; Lowery, D.L. Countering Cyber Threats to Financial Institutions. In *A Private and Public Partnership Approach to Critical Infrastructure Protection*; Springer: Berlin/Heidelberg, Germany, 2020.
82. Nifakos, S.; Chandramouli, K.; Nikolaou, C.K.; Papachristou, P.; Koch, S.; Panaousis, E.; Bonacina, S. Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors* **2021**, *21*, 5119. [CrossRef]
83. Das, S.; Siroky, G.P.; Lee, S.; Mehta, D.; Suri, R. Cybersecurity: The need for data and patient safety with cardiac implantable electronic devices. *Heart Rhythm* **2021**, *18*, 473–481. [CrossRef] [PubMed]
84. Bani Issa, W.; Al Akour, I.; Ibrahim, A.; Almarzouqi, A.; Abbas, S.; Hisham, F.; Griffiths, J. Privacy, confidentiality, security and patient safety concerns about electronic health records. *Int. Nurs. Rev.* **2020**, *67*, 218–230. [CrossRef] [PubMed]
85. Argaw, S.T.; Troncoso-Pastoriza, J.R.; Lacey, D.; Florin, M.V.; Calcavecchia, F.; Anderson, D.; Burleson, W.; Vogel, J.M.; O'Leary, C.; Eshaya-Chauvin, B.; et al. Cybersecurity of Hospitals: Discussing the challenges and working towards mitigating the risks. *BMC Med. Inform. Decis. Mak.* **2020**, *20*, 146. [CrossRef] [PubMed]
86. Kopp, E.; Kaffenberger, L.; Jenkinson, N. *Cyber Risk, Market Failures, and Financial Stability*; International Monetary Fund: Washington, DC, USA, 2017.
87. Maalem Lahcen, R.A.; Caulkins, B.; Mohapatra, R.; Kumar, M. Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity* **2020**, *3*, 10. [CrossRef]
88. Dupont, B. The cyber-resilience of financial institutions: Significance and applicability. *J. Cybersecur.* **2019**, *5*, tyz013. [CrossRef]
89. Joiner, K.F.; Tutty, M.G. A tale of two allied defence departments: New assurance initiatives for managing increasing system complexity, interconnectedness and vulnerability. *Aust. J. -Multi-Discip. Eng.* **2018**, *14*, 4–25. [CrossRef]
90. Mughal, A.A. The Art of Cybersecurity: Defense in Depth Strategy for Robust Protection. *Int. J. Intell. Autom. Comput.* **2018**, *1*, 1–20.
91. Progoulakis, I.; Rohmeyer, P.; Nikitakos, N. Cyber physical systems security for maritime assets. *J. Mar. Sci. Eng.* **2021**, *9*, 1384. [CrossRef]

92. Steingartner, W.; Galinec, D.; Kozina, A. Threat defense: Cyber deception approach and education for resilience in hybrid threats model. *Symmetry* **2021**, *13*, 597. [CrossRef]
93. Capodieci, N.; Sanchez-Adames, C.; Harris, J.; Tatar, U. The Impact of Generative AI and LLMs on the Cybersecurity Profession. In Proceedings of the 2024 Systems and Information Engineering Design Symposium (SIEDS), Charlottesville, VA, USA, 3 May 2024; pp. 448–453. [CrossRef]
94. Palmquist, A.; Jedel, I.; Goethe, O. Universal Design in Extended Realities. In *Universal Design in Video Games: Active Participation Through Accessible Play*; Springer: Berlin/Heidelberg, Germany, 2024; pp. 245–276.
95. Bicalho, D.R.; Piedade, J.M.N.; de Lacerda Matos, J.F. The Use of Immersive Virtual Reality in Educational Practices in Higher Education: A Systematic Review. In Proceedings of the 2023 International Symposium on Computers in Education (SIIE), Setubal, Portugal, 16–18 November 2023; pp. 1–5. [CrossRef]