information

MDPI

Article

Towards an Innovative Model for Cybersecurity Awareness Training

Hamed Taherdoost

College of Technology and Engineering, Westcliff University, Irvine, CA 92614, USA;
hamed.taherdoost@gmail.com; Tel.: +1-236-889-5359

Abstract: The rapid evolution of cybersecurity threats poses a significant challenge to organizations and individuals, necessitating strengthening defense mechanisms against malicious operations. Amidst this ever-changing environment, the importance of implementing efficacious cybersecurity awareness training has escalated dramatically. This paper presents the Integrated Cybersecurity Awareness Training (iCAT) model, which leverages knowledge graphs, serious games, and gamification to enhance cybersecurity training. The iCAT model's micro-learning module increases flexibility and accessibility, while real-time progress monitoring and adaptive feedback ensure effective learning outcomes. Evaluations show improved participant engagement and knowledge retention, making iCAT a practical and efficient solution for cybersecurity challenges. With an emphasis on adaptability and applicability, iCAT provides organizations in search of accessible and efficient cybersecurity awareness training with a streamlined approach.

Keywords: cybersecurity awareness training; innovative model; integrated framework; micro-learning module; serious games

1. Introduction

In contemporary society, cybersecurity assumes a critical function by safeguarding personal information, business and industrial data, intellectual property, and government information against cybercriminals and hackers. A direct correlation exists between the proliferation of technology and the escalation of cybercrime [1]. As the number of cyberattacks continues to skyrocket, the primary aim of cybersecurity is to safeguard information and reduce the likelihood of worldwide and calamitous repercussions [2,3].

Cybersecurity and preventing cyberattacks have been developing concerns for organizations for several years. The entities that are susceptible to cyberattacks encompass a wide spectrum, including major corporations and vital infrastructures. Higher education institutions, as reported by the UK Government in its 2022 Cyber Security Breaches Survey, were also subject to such incidents, with 62% encountering attacks or breaches every week [4].

Numerous prior studies have established that most cybersecurity incidents can be attributed to the behaviors and actions of individuals [5–7]. Human error is frequently recognized as a vulnerability in cybersecurity. Cybercriminals capitalize on human susceptibilities by employing social engineering strategies, specifically targeting ignorance or errors in judgment [8,9].

The perpetual predicament individuals and organizations encounter is the ever-evolving character of cyber threats. Constant innovation and adaptation of malicious actors' strategies necessitate an informed and proactive approach to cybersecurity [10,11]. Awareness training is of utmost importance as it provides individuals with the necessary knowledge and abilities to identify, alleviate, and react efficiently to these continuously evolving hazards [12]. Cybersecurity awareness training is an efficacious instrument that reinforces this interpersonal connection, cultivating an organization-wide ethos of vigilance regarding security that transcends individual hierarchies. Educating individuals regarding the dangers and repercussions of cyber threats enables them to defend against potential assaults actively [13].

check for updates

Citation: Taherdoost, H. Towards an Innovative Model for Cybersecurity Awareness Training. *Information* **2024**, *15*, 512. https://doi.org/10.3390/info15090512

Academic Editor: Willy Susilo

Received: 2 August 2024
Revised: 16 August 2024
Accepted: 21 August 2024
Published: 23 August 2024

The ramifications of a successful cyber-attack extend beyond the immediate financial losses experienced by organizations. Conspiracy-driven consequences of a security breach may include harm to an organization's reputation, legal ramifications, and declining consumer confidence. Therefore, organizations need to establish a security culture and reduce the potential vulnerabilities associated with human error by implementing a robust cybersecurity awareness program [14].

Despite numerous existing models, there is a lack of integration of adaptive learning paths and user-centric accessibility in cybersecurity training, which our proposed framework aims to address. By conducting an extensive review of relevant scholarly works, this article establishes the foundation for a nuanced comprehension of the present condition of cybersecurity awareness training. Detailed descriptions of the innovative model's design, strategies, and evaluation criteria will be provided. The objective is to identify the critical components of effective cybersecurity training systems and integrate these elements into a cohesive framework to enhance training outcomes.

This study aims to answer the question: "How can a new model for cybersecurity awareness training effectively enhance user engagement and knowledge retention?". This research makes the following key contributions:

- Development of the iCAT model integrating knowledge graphs and gamification.
- Introduction of a micro-learning module for enhanced flexibility.
- Implementation of real-time progress monitoring and feedback mechanisms.
- Comprehensive evaluation demonstrating increased engagement and knowledge retention.

The structure of this research study is as follows: The background section (Section 2) provides contextual information. The literature study in Section 3 explores the methodology used to choose articles, the progress made in cybersecurity, and the usefulness of gamification and serious games. A discussion is included in Section 3.3 after this. In Section 4, the suggested framework is presented, with an emphasis on the new micro-learning module. The study is finally concluded in Section 5 with some conclusions and suggestions for more research.

2. Background

Cybersecurity is a multifaceted issue that is substantially influenced by the actions of non-technical end-users when engaging with online content. Insufficient protection against online threats with technological countermeasures is uncommon due to security's dynamic and intricate nature. As an illustration, it is the duty of users to modify their privacy configurations, select robust passwords, and adhere to security protocols. Based on users' current understanding of online risks and the technology they employ, these choices necessitate foresight, informed decision-making, and the consideration of compromises [15–18].

Cybersecurity awareness is utilized to convey or distribute security obligations and proper conduct to individuals [19], thereby instilling in them a degree of doubt when confronted with unconventional or unusual circumstances [20]. It is not synonymous with comprehensive understanding; rather, it aims to draw individuals' attention to a security issue or collection of issues, prompting them to recognize their possible ramifications and take appropriate action [21]. It is disseminated via diverse communication channels, typically involving a condensed, less rigorous, and shortened duration compared to security education and training [22]. Typically, its endeavors target wide-ranging audiences, most of whom remain inactive recipients of the information. Cybersecurity awareness produces immediate, specific, and short-term learning unless the exercises are performed repeatedly [23].

In recent years, there has been a proliferation of evaluations that can be classified as program outcomes and outputs. These assessments serve as potential indicators of the efficacy of cybersecurity awareness initiatives. Numerous previous studies rely on the measurement and evaluation of one or more of the subsequent variables in order to ascertain the efficacy of a cybersecurity awareness program: the reduction in cybersecurity incidents that transpired after the implementation of the program; the alteration in the audience's perception, knowledge, attitude, and behavior; and the quantification of audience interest in cybersecurity awareness programs, typically expressed as the number of participants. While the initial parameter is straightforward and indicates whether the audience was pleased or dissatisfied with a cybersecurity awareness program, it needs to indicate whether the awareness program had a tangible impact in practical terms. Similarly, the second parameter cannot ascertain whether the decline in cybersecurity incidents that have affected the audience since implementing a more robust firewall and network protection system is attributable to a cybersecurity awareness program or another factor. Although complex, the third parameter is the most significant. It measures and evaluates the audience's changes in security-related knowledge, attitude, and conduct [24].

Before anything else, increasing awareness requires measuring it within each targeted group. Awareness measurements aim to assess cybersecurity awareness using a dependable methodology. Generally, awareness is assessed among an organization's workforce by amalgamating three distinct methodologies. Attitude, knowledge, and behavior are all assessed via questionnaires and surveys [25]. In security, behavior modeling is examined through survey-based research and model-driven approaches. This includes examining information-sharing, compliance with security policies [26], and computer security behavior during interaction with email attachments [27].

An effective cybersecurity awareness program should comprise sufficient training that aligns with the organization's goals, prioritizing enhancing employees' cybersecurity awareness. At the same time, they carry out their job responsibilities and facilitate interactive communication among all stakeholders regarding any cybersecurity-related issues. Similarly, awareness programs that fail to alter individuals' perceptions of cyber incidents and produce a positive effect on an organization may be deemed ineffective. A cybersecurity awareness program is a long-term investment for an organization that will contribute to developing a cybersecurity culture if training is provided consistently. An even more dynamic conception of the awareness objective transcends the mere prevention of cybersecurity incidents [28].

3. Literature Review

For the literature review, a systematic search was conducted on Scopus, spanning the period from 2019 to 30 December 2023. The search focused on the intersection of cybersecurity, awareness, and training, employing three specific queries: (1) "Cybersecurity (Title) AND awareness AND training (Title, Abstract, Keywords)", yielding 215 papers; (2) "Cybersecurity (Title) AND awareness AND learning (Title, Abstract, Keywords)", resulting in 167 papers; and (3) "Cybersecurity (Title) AND awareness AND education (Title, Abstract, Keywords)", producing 189 papers. These searches aimed to comprehensively cover literature related to cybersecurity awareness, including different aspects.

After removing duplicates from the 571 hits from the initial search, 380 unique papers remained. After that, 129 papers remained after filtering criteria were used to keep only original English articles and eliminate reviews, books, book chapters, and conference papers. Subsequent screening excluded publications that mostly presented case studies in favor of choosing those that explicitly proposed and evaluated a model or framework. A further filtering procedure produced 25 papers that were included for in-depth examination. The methodical selection of 25 papers from a literature review on cybersecurity awareness is shown in Figure 1, with a focus on models and frameworks.

The 25 articles address a variety of topics related to cybersecurity awareness training, including serious games, platforms like MaCySTe [29], novel models like PipCKG-BS [30], research on vulnerabilities like YOLOv5 [31], and serious games [32]. Additionally, they investigate frameworks, learning management system integrations, and simulations like SimPCNL [33], providing valuable insights and customized methods to the sector to solve various cybersecurity training concerns. A succinct overview of several cybersecurity awareness training papers is given in Table 1.

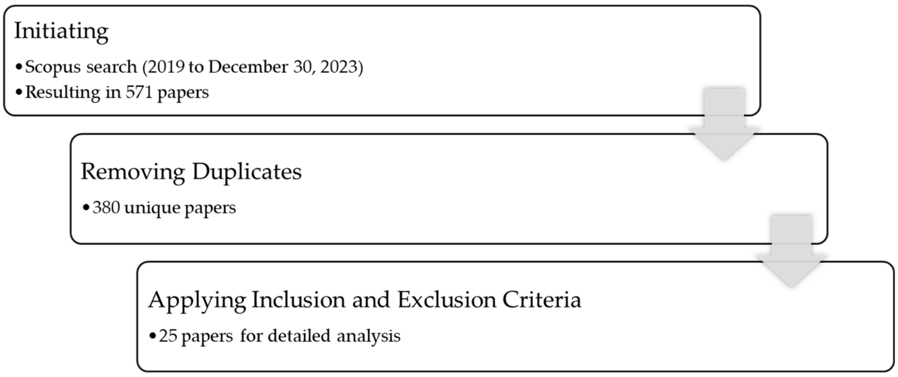
Initiating
• Scopus search (2019 to December 30, 2023)
• Resulting in 571 papers
Removing Duplicates
• 380 unique papers
Applying Inclusion and Exclusion Criteria
• 25 papers for detailed analysis

Figure 1. Selection process for model/framework evaluation.

Table 1. Summary of cybersecurity awareness training papers.

Study	Concepts Supporting the Model	Tool's Components	Context	Findings
[30]	PLMs, contextual features, prompt-based learning, NER, RE	Named entity recognition (NER), relation extraction (RE) models, PLMs	Blockchain systems	Outperforms advanced methods in CTI extraction for blockchain CKG.
[34]	Engaging and personalized experiences	Serious game for cybersecurity awareness	General cybersecurity	79% learned new things, 84% engaged, 68% had fun, 84% would recommend.
[35]	Real-time feedback, KSAs, Godot engine	SPL game, real-time feedback system, educational content tailored to user preferences	General cybersecurity	Crucial training tool, strong system usability (74.09%), inclusive content.
[29]	Reproducing network infrastructure, realistic testing	Open-source project, ship simulators, cybersecurity testing	Maritime cybersecurity	Realistic testing for cybersecurity in the maritime sector.
[31]	Adversarial attacks, transfer learning	YOLOv5 model, adversarial attack methods, parameter changes	AI cybersecurity, maritime systems	Raises awareness of AI algorithm vulnerability to attacks.
[36]	BiLSTM, neural network, tensor decomposition, self-distillation strategy	CSNT model, Pearson Mix Net	Penetration testing	CSNT has advantages for completing cybersecurity data in the knowledge graph.
[37]	Gamification, self-regulated learning	Gamified courses, Moodle integration	General cybersecurity	Supports self-regulated learning for cyberspace users.
[38]	Evolutionary game theory, cybersecurity investment strategies	Game theory model, replicator dynamics	Smart-home cybersecurity	Costs should be low for smart-home users, and rewards should be crucial for commitment.
[39]	Capture the Flag (CTF) competitions, educational challenges	Learning platform with CTF section, teacher, and competition modes	General cybersecurity	Proposed solution for cybersecurity knowledge, positive results.
[40]	Capability evaluation, security management	CAT framework, case studies	Remote working cybersecurity	Three levels, 25 core practices, effective in real-world settings.

Table 1. *Cont.*

Study	Concepts Supporting the Model	Tool's Components	Context	Findings
[41]	HIL technology, real sensors, and actuators	WonderICS, G-ICS, APT demonstrator, real industrial control devices	Industrial control systems (SCADA)	Platforms for awareness and training in SCADA cybersecurity.
[42]	SETA framework, interactive video game	Cyber shield game, threat scenarios, pre-game and post-game surveys	General cybersecurity	Interactive game improves cybersecurity awareness by 51.4%.
[43]	Continuous improvement, curriculum integration	Cybersecurity Awareness Framework, policy and procedure development	Academia	Improves cybersecurity awareness among university graduates.
[44]	Place management techniques, anti-phishing training	Anti-phishing training program	General cybersecurity	Positive impact of anti-phishing training on reducing cybercrime.
[45]	SDN, real-time awareness, ML-based IDS	Situational awareness framework, neural network, SDN paradigm	General cybersecurity	Increases prediction accuracy by more than 4%.
[32]	Cost–benefit analysis, CSAT program types	Theoretical framework for cost–benefit analysis, CSAT program categorization	General cybersecurity	Transforms physical escape room into virtual setting with positive immersion.
[46]	Escape room game, immersive learning	Virtual escape room, cybersecurity challenges for SMEs	SMEs	SYNAPSE successfully identifies security-related tweets with high accuracy.
[47]	Twitter-based threat monitoring, IoCs	SYNAPSE system, tweet-processing pipeline, feature extraction, binary classification, clustering strategy	Social media monitoring, IT infrastructure	Raises industry software developers' awareness of secure coding.
[48]	Secure coding guidelines, AI-guided hints	Sifu platform, automatic challenge assessment, AI coach	Industry software development	Positive responses and increased understanding of cybersecurity concepts.
[49]	AR technology, active learning	CybAR game, mobile application, AR feedback	General cybersecurity	Aids in developing and assessing cybersecurity competencies during exercises.
[50]	Hybrid exercises, formative assessment, ARCS model	Competence development framework, assessment stages, hybrid CDX	General cybersecurity	Applicable to actual training activities.
[51]	LMS integration, SCORM format	CyLMS system, Moodle integration, standard interfaces for training management	General cybersecurity	App significantly increases participant performance by almost 20%.
[33]	ARCS model, elementary education	Learning Content Management System (LCMS), mobile app, suite of quick games	Elementary education	Reliable and versatile in percutaneous renal access surgical training.
[52]	AR technology, medical simulation	SimPCNL simulator, visual–haptic environment, clinical database	Medical cybersecurity	CATRAM is designed for different organizational audiences with specific content and objectives.
	Awareness methodologies, targeted training content	CATRAM model, organizational training	General cybersecurity	

Recently, a growing emphasis has been placed on creating novel cybersecurity awareness training methods. Scholars have investigated diverse approaches to augment individuals' comprehension and readiness to confront dynamic cyber hazards. Li et al. [30] contributed significantly by introducing PipCKG-BS, a pipeline-based method for building a reliable cybersecurity knowledge graph (CKG) especially suited for blockchain systems. This innovative approach achieves superior performance in extracting and organizing critical cyber threat intelligence (CTI) information by utilizing cutting-edge techniques like named entity recognition (NER) and relation extraction (RE), as well as contextual features and pre-trained language models (PLMs).

This method tackles the critical requirement for effective knowledge graph generation in blockchain, where complicated cybersecurity data necessitates advanced techniques. PipCKG-BS demonstrates how cutting-edge methods such as NER and RE, in conjunction with contextual features and PLMs, can produce high-quality CKGs that greatly increase cybersecurity awareness [30].

3.1. Cybersecurity Advancements

Researching SCADA (Supervisory Control and Data Acquisition) systems, Puys et al. [41] suggested hardware-in-the-loop platforms for training and raising cybersecurity awareness. WonderICS and G-ICS use hardware-in-the-loop (HIL) technology to imitate industrial situations realistically. Running the firmware of genuine devices without physical hardware is made possible by incorporating firmware emulation. This creative method closes the gap in critical infrastructure protection by giving complete training and awareness demonstrations for SCADA cybersecurity.

A machine learning-based cybersecurity situational awareness framework was presented by Nikoloudakis et al. [45] and implemented in Software-Defined Networking (SDN). The framework leverages SDN's real-time awareness capability to identify and evaluate network-enabled items in real-time. Prediction accuracy is increased by using neural networks trained on heterogeneous data. A real-world evaluation of the system showed a 4% increase in total prediction accuracy, demonstrating the potential of machine learning to improve cybersecurity situational awareness.

Zhang et al. [53] investigated cybersecurity awareness training initiatives concurrently using a framework for cost–benefit analysis. Their analysis divided programs into four categories—negligible, consistent, rising, and diminishing—based on benefits and three categories—constant, complementary, and compensatory—based on expenses. The results emphasized how different program advantages contribute to preserving, improving, or decreasing an organization's security posture. This nuanced viewpoint helps businesses optimize the trade-off between cost and security and customize cybersecurity awareness initiatives to their unique needs.

Moreover, SYNAPSE, a Twitter-based streaming threat monitor, was suggested by Alves et al. [46] to raise cybersecurity awareness. This creative method analyzes tweets to produce a dynamic overview of a monitored asset's threat landscape. With a true positive rate of over 90%, SYNAPSE effectively recognized tweets about security while offering pertinent and timely summaries of possible dangers. A modern and thorough approach to cybersecurity awareness is demonstrated by incorporating social media data into threat monitoring.

3.2. Serious Games and Gamification for Effective Cybersecurity Awareness

Enhancing cybersecurity awareness and training using gamification and serious games is a dynamic and successful technique. Hodhod et al. [34] presented CyberHero, an adaptive serious game whose purpose is to assess how well it raises awareness of cybersecurity issues. Positive results were obtained from the game's captivating story, as reported by 79% of players who learned new information. A total of 84% of participants thought the backstory was interesting, 68% said the gameplay was enjoyable, and 84% said they would suggest the game to friends. These findings highlight the potential of serious games to provide an interesting and pleasurable learning environment in addition to dispensing knowledge.

Sharif and Ameen [35] created the Security Power Lab (SPL), a serious game that provides personalized content, real-time feedback, and an immersive experience in a similar spirit. SPL was rated a useful training tool for enhancing cybersecurity knowledge and skills, with a system usability score of 74.09%. The game's position in serious games for cybersecurity training is further cemented by its inclusivity in customizing content to each user's preferences, abilities, and knowledge.

Abu-Amara et al. [42] introduced a SETA-based gamification framework with an interactive video game named Cyber Shield, moving toward creative frameworks and gamification tactics. The game showed a 51.4% increase in workers' cybersecurity awareness across levels of password complexity, social engineering, phishing assaults, and physical security. This gamified approach outperformed conventional techniques by offering an interactive and captivating platform for cybersecurity training.

With their conceptual Cybersecurity Awareness Framework for Academics, Khader et al. [43] contributed to this field. This framework is centered on enhancing cybersecurity knowledge integration in university courses. Its focus on creating, incorporating, distributing, and evaluating cybersecurity information provides educational institutions with a model for raising graduate awareness. This all-encompassing strategy ensures a constant and changing process of cybersecurity education by aligning with the dynamic nature of cyber threats.

3.3. Discussion

The effectiveness of cybersecurity awareness training programs as they are now implemented is hampered by several issues. Many training programs take a one-size-fits-all approach and lack customization [30,34]. This restriction might make it more difficult for individuals to participate and comprehend because it disregards their unique learning preferences and current knowledge bases. Moreover, investigations by Longo et al. [29] and Lee et al. [31] have shown that static content and inadequate real-world simulation lead to knowledge gaps by falling behind the quickly changing cybersecurity scene because static content can easily become outdated and inform users about new risks and defenses.

Traditional training approaches still need help with engagement and interactivity, and some programs need the dynamic components required for participants to participate actively. The findings of Douha et al. [38] and Sharif and Ameen [35], which highlight the significance of individualized and interesting experiences for successful cybersecurity training, serve as examples of this. Wang et al. [36] expressed concern that the lack of established measurements makes it difficult to measure effectiveness and evaluate the long-term effects of programs. Resource limitations, employee reluctance, and compliance issues make these obstacles even more difficult, especially for small and medium-sized businesses. These findings are consistent with those of Hijji and Alam [40] and Ortiz-Garces et al. [39]. Future cybersecurity awareness training programs should emphasize personalization, dynamic information, and more interactivity to solve these issues. They should be modeled after cutting-edge models like PipCKG-BS, CyberHero, and Security Power Lab. MaCySTe and the YOLOv5 vulnerability assessment prove that integrating real-world simulations can offer useful insights into cybersecurity scenarios. According to Wang et al., standardized parameters for measuring are essential for evaluating long-term efficacy. Furthermore, as shown by Ortiz-Garces et al. [39] and Hijji and Alam [40], overcoming resource limitations and cultivating an involvement culture will be critical to the success of upcoming training projects.

4. Proposed Framework

It is frequently difficult for traditional cybersecurity training to keep participants interested, personalized, and flexible enough to accommodate different learning preferences. Acknowledging these difficulties, iCAT integrates tried-and-true elements that have shown effectiveness in earlier frameworks to transform cybersecurity awareness. iCAT creates a strong and adaptable basis by fusing serious games, knowledge graphs, gamification, learning management systems, and CTF challenges.

4.1. Design

Proven elements from popular cybersecurity awareness frameworks are seamlessly integrated into the Integrated Cybersecurity Awareness Training (iCAT) framework. Each integrated component adds a special dimension to create a thorough and productive training environment. The iCAT framework's integrated design process is depicted in Figure 2, which combines gamification, knowledge graph utilization, serious game development, CTF component, and micro-learning modules into a unified cybersecurity awareness training method. Figure 2 illustrates how these elements work together to form a training system that is coherent. The adaptive learning paths ensure that training is personalized to individual learners' pace and comprehension. In contrast, user-centric accessibility ensures that all users, regardless of their technical proficiency, can benefit from the training.

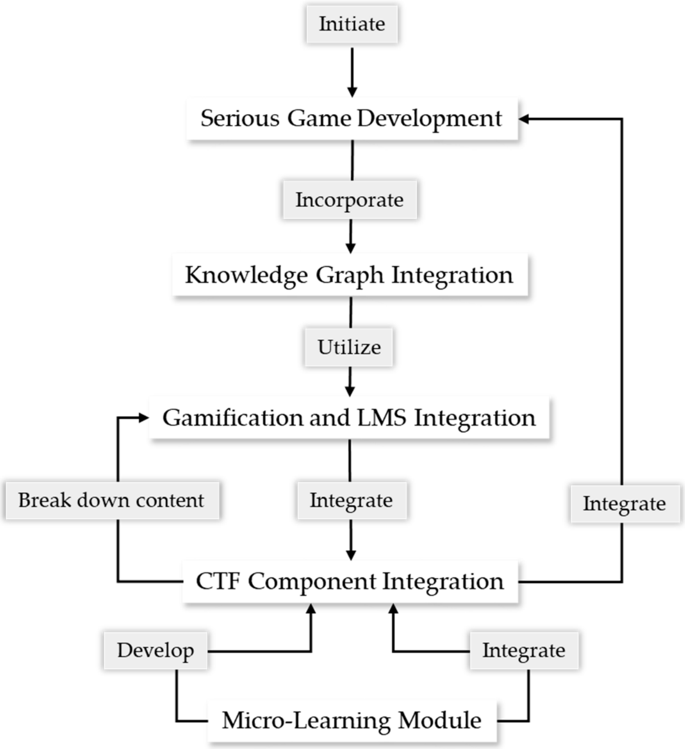

Figure 2. Design steps for the iCAT framework.

4.1.1. Serious Game Component

Inspired by the popularity of the CyberHero serious game [34], the iCAT framework's Serious Game Component is a ground-breaking educational tool. With the help of gamification components, this adaptive program turns conventional cybersecurity training into an exciting adventure that encourages engagement and individualized learning. The adaptive algorithms of the component dynamically adjust tasks according to each participant's success, guaranteeing a personalized and demanding experience that corresponds with their ability level. According to CyberHero's success, real-world cybersecurity scenarios immerse users in real-world challenges and promote a thorough grasp of potential threats and weaknesses.

Extending the ideas found in CyberHero, iCAT incorporates the gamification components that worked well to keep participants interested. The Serious Game Component keeps its gamified features, effective learning prompts, and captivating backstory to improve participant motivation and immersion. By adapting CyberHero's successful aspects, iCAT guarantees a consistent and efficient method for raising cybersecurity awareness through serious gaming. This integration keeps participants interested in the always-changing cyberspace and makes it easier to move from theoretical understanding to real-world application.

There are numerous advantages to the Serious Game Component of iCAT. Embedded gamification components raise motivation and participation and guarantee that participants stay interested over time. Reinforcing learning outcomes, the practical application of information in real-world circumstances bridges the gap between theory and practice. Furthermore, because the game is adaptive, players can advance at their own speed and create customized learning routes based on their ability levels. The Serious Game Component of the iCAT Framework is used in an integrated and useful way to improve participant engagement and individualized learning, as shown in Figure 3. This diverges into Engaging Story and Real-World Scenarios and Gamification and Adaptive Module before coming together at Seamless Integration and Consistent Approach. With an arrow looping back to the core box, this central element relates to Shapes Participants, Personalized Learning Paths, Adaptive Progression, and Elevated Motivation and Practical Application of Knowledge. This demonstrates how various components work together to produce a flexible and interesting learning environment.

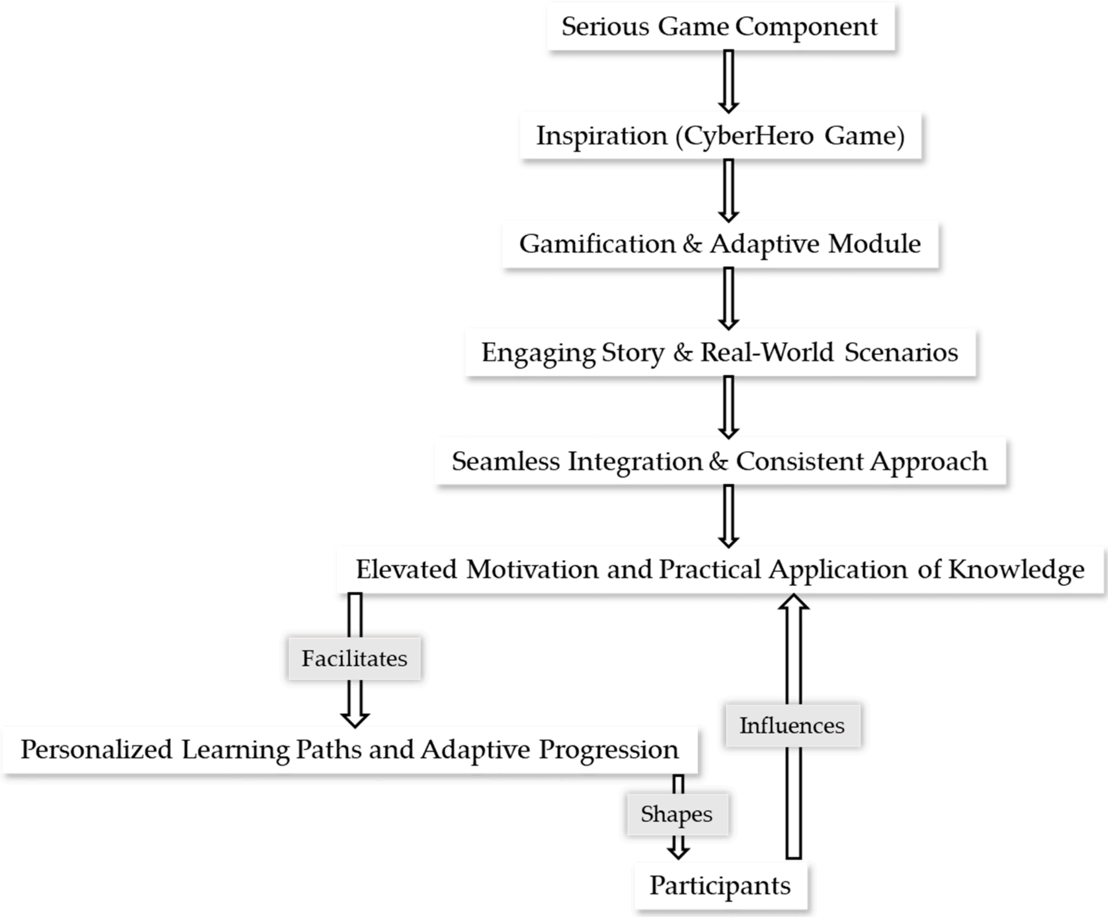
Serious Game Component
Inspiration (CyberHero Game)
Gamification & Adaptive Module
Engaging Story & Real-World Scenarios
Seamless Integration & Consistent Approach
Elevated Motivation and Practical Application of Knowledge
Facilitates
Influences
Personalized Learning Paths and Adaptive Progression
Shapes
Participants

Figure 3. iCAT framework—serious game integration.

4.1.2. Knowledge Graph Component

Understanding that cybersecurity training requires organized data, it incorporates the idea of a cybersecurity knowledge graph (CKG) [30]. Contextual characteristics and pre-trained language models (PLMs) are added to this component to improve its accuracy in extracting and organizing data from cyber threat intelligence (CTI). While PLMs improve the performance of named entity recognition (NER) and relation extraction (RE) models, improving the accuracy and efficiency of the information extraction process, contextual features enrich the CKG by adding metadata about cybersecurity concepts.

The Knowledge Graph Component is a dynamic resource that provides participants with an organized and integrated view of cybersecurity information throughout the learning experience. Participants gain from a well-structured knowledge base that makes it easier for them to traverse and comprehend challenging cybersecurity subjects. Incorporating modern NER and RE algorithms ensures accurate entity and relationship identification within the CKG. In order to navigate the constantly changing world of cyber dangers, participants need to have a deeper and more practical understanding of cybersecurity topics, which is fostered through interaction with the CKG. Figure 4 shows how users interact with the Knowledge Graph Component to develop a thorough comprehension of related cybersecurity ideas using sophisticated named entity recognition and relation extraction algorithms. In addition to contributing to Structured Information Retrieval and Advanced named entity recognition and relation extraction (RE) Techniques, this component dynamically navigates and comprehends an interconnected view of cybersecurity information. These processes enhance the interconnected view, which in turn engages participants and helps them gain a comprehensive understanding of cybersecurity concepts.

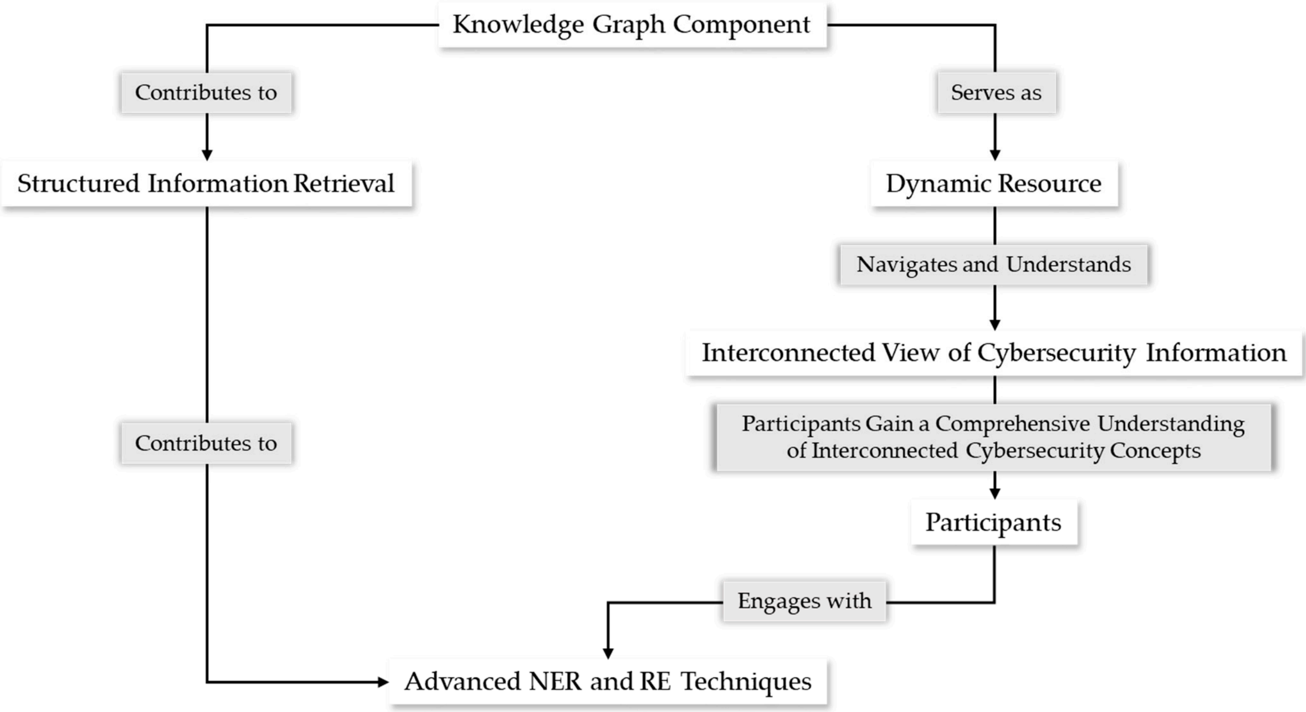
Knowledge Graph Component
Contributes to
Serves as
Structured Information Retrieval
Dynamic Resource
Navigates and Understands
Interconnected View of Cybersecurity Information
Contributes to
Participants Gain a Comprehensive Understanding of Interconnected Cybersecurity Concepts
Participants
Engages with
Advanced NER and RE Techniques

Figure 4. Knowledge Graph Component interaction in cybersecurity training.

The Knowledge Graph Component makes training materials more adaptive and relevant to changing threats and scenarios. When paired with cutting-edge NER and RE approaches, its function in structured information retrieval greatly enhances the efficacy and efficiency of knowledge dissemination and information extraction.

4.1.3. Gamification and Learning Management System

Based on the Gamification-Based Course [37], CyLMS [50], and the Serious Game Component [34], the gamification and Learning Management System component of the iCAT framework seamlessly combines components from successful models. This integration aims to improve training efficacy overall, participant motivation, and engagement. By implementing gamification concepts, iCAT turns the training process into an engaging and dynamic game-like environment by introducing game mechanisms like leaderboards, badges, and point systems. By creating an engaging and rewarding learning environment, these components—derived from the Gamification-Based Course—hope to increase participant immersion and retention of cybersecurity topics.

A strong Learning Management System modeled after CyLMS's accomplishments forms the core of iCAT's organizational structure. The Learning Management System, centralized and designed with cybersecurity awareness in mind, guarantees participant progress tracking, streamlined content distribution, and effective management of training resources. Similar to features in the Serious Game Component, real-time monitoring tools help instructors keep tabs on student accomplishments, engagement levels, and completion rates. The Learning Management System enables a methodical and well-structured training program, giving users quick access to educational materials and customized tests that are tailored to the particular difficulties and goals of cybersecurity training.

Furthermore, gamification and Learning Management System integration in iCAT go beyond solitary learning scenarios. iCAT encourages collaborative learning opportunities within the gamified framework, drawing inspiration from the collaborative nature of the Platform for Learning Cybersecurity. Enhancing the social aspect of learning, participants can participate in group challenges, exchange thoughts, and work together to address cybersecurity problems. The Serious Game Component inspired the real-time feedback mechanism, which ensures that participants receive feedback immediately on their accomplishments and opportunities for growth. Table 2 overviews the key components, models/strategies, instruments, and metrics for the iCAT framework's Gamification and Learning Management System component.

Table 2. Integrated gamification and Learning Management System model.

Element	Strategy	Implementation Tools	Evaluation Metrics
Gamification Elements	Game Mechanics Model	Gamification platform, Point system algorithm	Participation rates, Points earned, Leaderboard rankings
	Narrative Design Model	Storyboarding tools, Scenario creation software	Participant engagement, Story progression assessment
Learning Management System	User-Friendly Interface Model	Learning Management System platform (e.g., Moodle, Canvas)	Usability feedback, Navigation efficiency, and User satisfaction surveys
	Content Delivery Model	Content management system, SCORM compliance	Content completion rates, Timely delivery assessment
	Progress Tracking Model	Learning analytics tools, Progress tracking features	Completion rates, Time spent on modules, Assessment scores
	Collaborative Learning Model	Collaboration tools (e.g., forums, chat), Group project platforms	Forum participation, Group project completion, Peer assessment scores
Integration Approach	Holistic Integration Model	Custom integration scripts, API connections	Integration efficiency, Data consistency, User experience

4.1.4. Capture the Flag (CTF) Component

By incorporating successful elements from the study by Ortiz-Garces et al. [39], the CTF component of the iCAT framework seamlessly integrates practical cybersecurity challenges. By capitalizing on the competitive and interactive characteristics of CTF activities, iCAT augments its participants' abilities and practical implementation of theoretical knowledge. Consistent with the micro-learning module, the CTF component facilitates a transition for participants from the fundamental knowledge acquired via serious games and knowledge graphs to the practical challenges that require active engagement.

Using this interactive learning environment, practical skills vital for recognizing and mitigating potential hazards are refined, and theoretical concepts are reinforced. The challenges are situated within wider objectives for cybersecurity awareness training, guaranteeing that participants are involved in situations specifically pertinent to their educational goals. The CTF element provides an all-encompassing and adaptable learning environment by collaborating effectively with other components, including serious games and gamification. Furthermore, the competitive advantage of CTF activities inspires individuals to consistently improve their abilities, cultivating a proactive attitude towards cybersecurity risks.

Including feedback mechanisms within the CTF component allows participants to monitor their progress by providing real-time insights into their performance. Participants are duly informed regarding their strengths and areas that require further development using this feedback cycle. In addition, incorporating performance monitoring into the overarching Learning Management System provides a thorough evaluation of the progress made by the participants. The CTF challenges have been intentionally crafted to correspond with the micro-learning module, promoting a smooth progression from theoretical comprehension to hands-on implementation.

4.1.5. Enhanced Flexibility through Micro-Learning

The micro-learning module segments information into bite-sized, manageable units to improve retention and engagement. Acknowledging the intrinsic difficulties in retaining knowledge and making cybersecurity training accessible, the iCAT architecture presents a novel micro-learning module. This cutting-edge element is carefully crafted to move around roadblocks found in current frameworks, giving participants a customized and adaptable learning environment. The iCAT framework's micro-learning module is distinguished by its deliberate division of content into manageable modules, provision of adaptive learning pathways for customized experiences, and guaranteeing user-centric accessibility. Together, these features augment the effectiveness and accessibility of cybersecurity training (Table 3). It is feasible to help participants comprehend and remember important cybersecurity topics by breaking the training material into digestible segments. Because of the module's flexibility, users can progress at their own pace, meeting a range of timetables and rates of development. There is also an emphasis on accessibility, because the module provides brief, targeted lessons that make it easier for learners to understand cybersecurity education.

Table 3. Micro-learning module features in the iCAT framework.

Micro-Learning Module Component	Segmentation into Bite-Sized Modules	Adaptive Learning Paths	User-Centric Accessibility
Bite-sized Content	✔		
Personalized Learning		✔	
Interactive Delivery			✔

By drawing inspiration from the Serious Game Component of CyberHero [34], iCAT recognizes the necessity for a solution that promotes the long-term retention of knowledge. The micro-learning module simplifies intricate cybersecurity principles into concise, targeted modules. This methodology guarantees that participants are presented with information in manageable segments, augmenting their capacity to comprehend and retain crucial insights.

By incorporating the principles of gamification and the Learning Management System, iCAT endeavors to enhance the accessibility of cybersecurity training. The micro-learning module grants users immediate access to succinct instructional modules, allowing them to independently progress through the subject matter. The capacity to alter caters to various learning styles and schedules, thereby promoting a training experience that is more inclusive and focused on the learner.

Expanding upon the achievements of gamification tactics, the micro-learning module integrates components that augment the motivation and involvement of participants. Concise and targeted modules offer participants attainable milestones, fostering a feeling of achievement. Implementing gamified components, including progress monitoring and incentives, enhances motivation to maintain a steady commitment to the training material.

In order to strengthen the theoretical understanding gained from the micro-learning lodule, iCAT effectively incorporates practical, hands-on experiences that draw inspiration from the CTF component. Through CTF challenges, participants can implement the micro-learned concepts in real-world scenarios. This integration reinforces learning by bridging the divide between theoretical comprehension and practical implementation.

Through implementing the micro-learning module, iCAT embraces a learner-centric approach to instruction. The participants are granted the independence to traverse the modular content at their own pace, specifically emphasizing areas that pique their interest or are pertinent to their respective duties. Implementing this learner-centric model enables individuals to take charge of their education by customizing and adapting the training process to suit their specific requirements and inclinations. The iCAT micro-learning module workflow is depicted in Figure 5. It includes module selection, evaluation, and feedback stages, all of which contribute to providing a customized cybersecurity training experience.

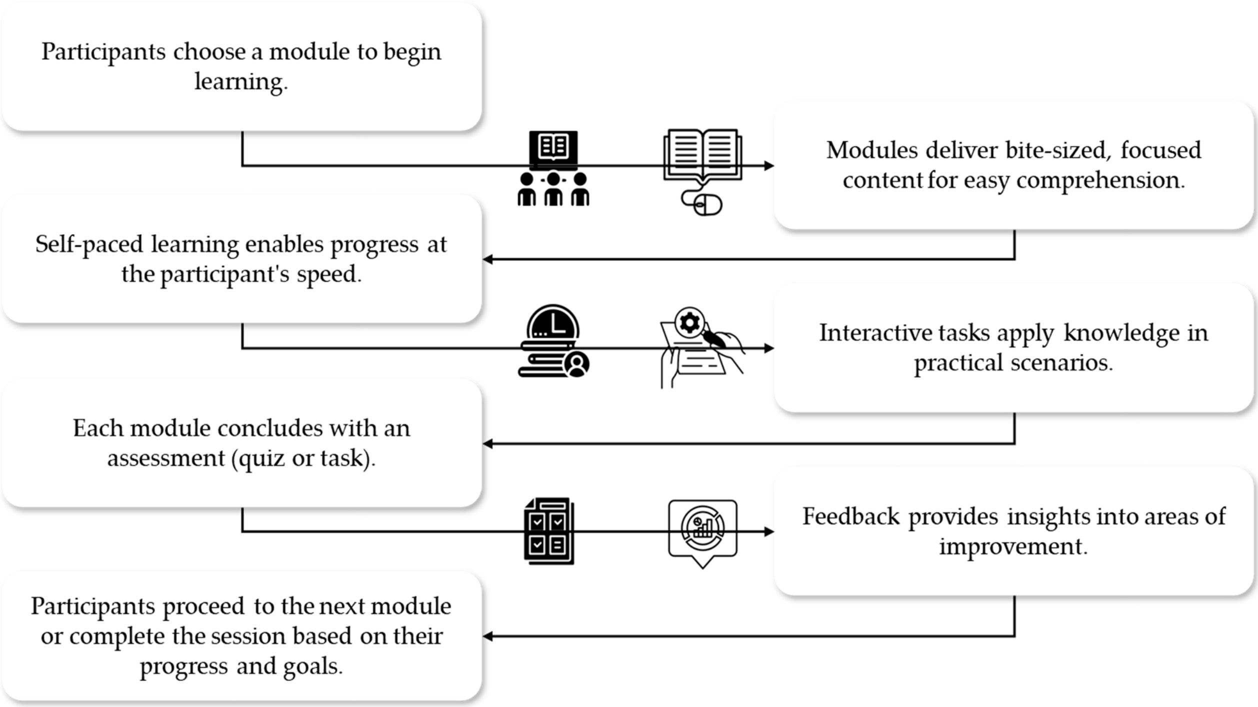
Participants choose a module to begin learning.
Modules deliver bite-sized, focused content for easy comprehension.
Self-paced learning enables progress at the participant's speed.
Interactive tasks apply knowledge in practical scenarios.
Each module concludes with an assessment (quiz or task).
Feedback provides insights into areas of improvement.
Participants proceed to the next module or complete the session based on their progress and goals.

Figure 5. Micro-learning module workflow.

5. Implications

Separately proven components are combined in the iCAT framework to produce a complete and successful cybersecurity training program. The iCAT framework includes a Serious Game Component, Knowledge Graph Component, gamification and learning management system, CTF Component, and micro-learning module. Every element adds special advantages to the framework, improving participants' learning results and participation (Figure 6). This integrated approach aims to enhance both practical skills and theoretical understanding, making cybersecurity training more effective and engaging. To improve comprehension, the Knowledge Graph Component uses methods like named entity recognition and relation extraction to organize and structure cybersecurity knowledge. To encourage and involve students, the gamification and learning management system component has features like leaderboards, badges, and point systems. The CTF Component offers real-time feedback, competitive challenges in a practical setting, and an environment that encourages the application of theoretical knowledge. The multifaceted approach not only addresses the urgent need for enhanced cybersecurity awareness, but also fosters a more profound comprehension of intricate concepts, thereby equipping individuals to more effectively navigate the changing digital landscape [54,55].

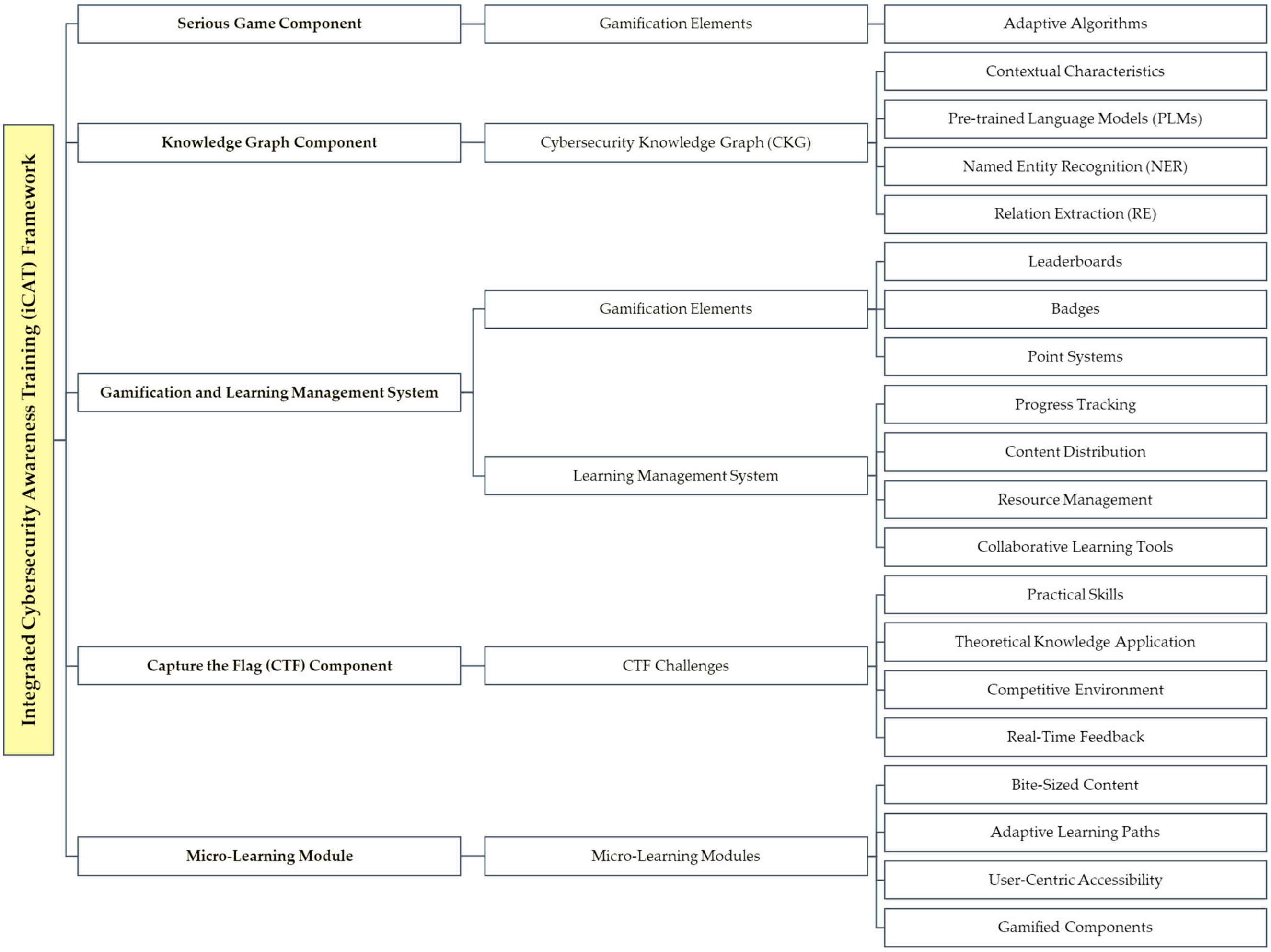
Integrated Cybersecurity Awareness Training (iCAT) Framework
Serious Game Component
Gamification Elements
Adaptive Algorithms
Contextual Characteristics
Knowledge Graph Component
Cybersecurity Knowledge Graph (CKG)
Pre-trained Language Models (PLMs)
Named Entity Recognition (NER)
Relation Extraction (RE)
Leaderboards
Gamification Elements
Badges
Point Systems
Gamification and Learning Management System
Progress Tracking
Content Distribution
Learning Management System
Resource Management
Collaborative Learning Tools
Practical Skills
Theoretical Knowledge Application
Capture the Flag (CTF) Component
CTF Challenges
Competitive Environment
Real-Time Feedback
Bite-Sized Content
Adaptive Learning Paths
Micro-Learning Module
Micro-Learning Modules
User-Centric Accessibility
Gamified Components

Figure 6. iCAT framework.

Learning experiences can be improved, and student engagement has been demonstrated by serious games like those that use augmented reality (AR) technologies [56]. These games aim to offer immersive, interactive activities that promote learning through satisfying, emotionally compelling encounters [57,58]. Since cooperative gameplay is crucial to improving both technical knowledge and soft skills like communication and strategic thinking, serious game development has shifted to prioritize team-centric approaches [59]. Game components like points, badges, and leaderboards help gamification—that is, increase motivation, engagement, and information retention—among students [60,61]. Combining successful models like the Gamification-Based Course and CyLMS will help educational institutions build a dynamic and interactive learning environment that promotes student engagement, skill development, and general academic achievement. Gamification components included in LMS can transform conventional teaching strategies and support inclusive and exciting learning environments for every learner. Using adaptive gamification components from the CyberHero game, the iCAT framework's Serious Game Component improves traditional cybersecurity training by providing interesting, customized, and pragmatic learning opportunities. While tracking progress, managing resources, and improving social learning via forums and chat for a well-structured program, the Gamification and Learning Management System component blends game mechanics from models like the Gamification-Based Course and CyLMS with LMS functionalities offering leaderboards, badges, and points for an interesting training environment. Studies indicate that gamification not only improves motivation but also improves the overall learning experience, resulting in improved academic outcomes [62,63]. Nevertheless, the potential of gamification is clear; however, it is imperative to conduct ongoing research to gain a comprehensive understanding of its long-term effects and to resolve any implementation obstacles [64].

In cybersecurity, knowledge graphs combine disparate and scattered data to enable the investigation of links between many entities and provide in-depth analysis [65]. These graphs are built by extracting structured ontology from scientific publications, including latent patterns and observable information, using hierarchical and semantic non-negative matrix factorization, and generating a multi-modal knowledge graph particular to the cybersecurity domain [66]. Knowledge graphs are not limited to cybersecurity, as seen by the German Tourism Knowledge Graph, which combines travel-related data from many sources to provide a well-chosen knowledge base for several uses [67]. Knowledge graph optimization improves the prediction of correlations between goods, vulnerabilities, and cybersecurity domain weaknesses. For example, the threat knowledge graph aggregating data from common threat databases improves the prediction of associations between products, vulnerabilities, and cybersecurity domain weakness [68].

By combining useful tasks that improve participants' abilities and application of theoretical information, the CTF component significantly contributes to cybersecurity education [69–72]. These challenges offer a progressive learning curve that lets students grasp difficult vulnerabilities and create advanced exploits, expanding their cybersecurity knowledge [69]. Using open-source tools helps maximize CTF events by providing participants with effective, scalable, and interesting experiences, improving the whole learning process [70]. Studying human behavior during CTF games can offer insightful analysis of decision-making processes, behaviors, and personal traits, thereby helping to blame and disrupt attackers [72] more accurately. Including CTF in cybersecurity training courses, including the DICYSTECH project, allows students to evaluate their competencies, monitor their development, and hone their cybersecurity skills using practical experiences in realistic virtual environments [71].

Using micro-learning modules breaks down knowledge into easily digestible bits, therefore providing a disciplined and succinct method of instruction. These courses have been extensively used in many fields, improving retention and involvement by concentrating on particular materials without overwhelming the students. Particularly in cybersecurity training, the research on the application of micro-credentials in professional education systems [73] emphasizes the need for flexible and adaptive programs that satisfy the needs of the labor market, so aligning to address issues in knowledge retention and accessibility. Combining these strategies will help cybersecurity training be improved using bite-sized, interesting courses encouraging effective learning and retention.

6. Future Research

Although thorough and all-encompassing, the iCAT framework requires empirical validation to confirm its effectiveness and applicability in several environments. More research helps to improve the structure and influence of cybersecurity education.

Future research will mostly concentrate on thorough surveys and assessments. These surveys will gather both qualitative and quantitative information from those with iCAT-training. The evaluation will include user involvement, knowledge retention, skill application, and training satisfaction will be evaluated. This information aids in the identification of strengths and shortcomings of frameworks.

Proof of the iCAT framework's effectiveness depends on thorough empirical research. The performance and retention of iCAT and conventional training methods are compared using controlled assessments. Post-training assessment results, long-term memory, and practical skill application will all affect the framework's efficacy. Testing the framework's adaptability through demographics like technical skill and age is vital.

Future studies must look at the scalability and adaptability of the iCAT paradigm. Scholars must assess the structure of small businesses, big companies, and other sectors. Implementation calls for technical support and interface simplicity with current cybersecurity training initiatives. Finding scalability and flexibility helps one to create frameworks that make it successful and accessible for a large audience.

Future studies on advanced technology integration into the iCAT framework are underlined. Artificial intelligence and machine learning techniques could dynamically modify material depending on real-time performance data to customize training. VR and AR could make CTF challenges and realistic, engaging, serious games more appealing.

Longitudinal studies are required to ascertain the long-term effects on cybersecurity awareness and behavior of the iCAT architecture. Participants in this research will be tracked over time to find out how faithfully they apply framework information and skills. These studies will help to hone the long-term efficacy framework. The iCAT framework will be developed and refined, in part by multidisciplinary cooperation. Experts in cybersecurity, psychology, and education can assist in creating improved training courses. Group studies might offer fresh technology and training approaches to enhance the experience.

7. Conclusions

An examination of twenty-five papers about cybersecurity awareness training has unveiled a heterogeneous array of pioneering methodologies. The effectiveness of gamification and serious games in fostering participant engagement and knowledge retention has been demonstrated using CyberHero. Incorporating AI techniques and knowledge graphs, such as PipCKG-BS, has enhanced the organization and extraction of data in cybersecurity. Practical training platforms, such as CTF and virtual testbeds, enhance hands-on experiences and equip individuals with the necessary skills to tackle authentic cybersecurity situations (MaCySTe). Further investigation into integrating micro-learning modules and adaptive learning strategies may provide viable solutions to the difficulties associated with content retention and comprehension.

The proposed iCAT framework expands upon these discoveries by providing a comprehensive and flexible methodology. Through integrating effective elements from multiple frameworks, iCAT offers a comprehensive training experience. By integrating serious games, knowledge graphs, and micro-learning, both engagement and adaptability can be significantly increased. However, potential obstacles include the resource demands for hosting and maintenance and the complexity of integrating diverse components seamlessly. Although the modular design facilitates flexibility, participants may encounter a period of adjustment as they become accustomed to the framework's various components.

Future studies on the iCAT framework will focus on how well it works in various organizational contexts and how it affects participant engagement, knowledge retention, and skill application in real-world situations. Its ongoing growth will also be aided by investigating ways to map participants' cybersecurity competency development and modify the framework to fit various organizational and cultural situations. Our future work will include conducting surveys and evaluating the proposed framework to ensure it is effective and flexible in various settings. It will empirically validate the framework through rigorous evaluation methodologies.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The author declares no conflicts of interest.

References

1. Bossler, A.M.; Berenblum, T. Introduction: New directions in cybercrime research. *J. Crime Justice* **2019**, *42*, 495–499. [CrossRef]
2. Taherdoost, H. An overview of trends in information systems: Emerging technologies that transform the information technology industry. *Cloud Comput. Data Sci.* **2023**, *4*, 1–16. [CrossRef]
3. Khan, M.A.; Merabet, A.; Alkaabi, S.; El Sayed, H. Game-based learning platform to enhance cybersecurity education. *Educ. Inf. Technol.* **2022**, *27*, 5153–5177. [CrossRef]
4. Prümmer, J.; van Steen, T.; Berg, B.v.D. A systematic review of current cybersecurity training methods. *Comput. Secur.* **2024**, *136*, 103585. [CrossRef]
5. Lab, K. *The Human Factor in IT Security: How Employees Are Making Businesses Vulnerable from within*; Kaspersky Daily: Moscow, Russia, 2018.
6. Williams, S. *More than Half of Personal Data Breaches Caused by Human Error*; IT Brief: Melbourne, Australia, 2019.
7. Hadlington, L. Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon* **2017**, *3*, e00346. [CrossRef] [PubMed]
8. Okechukwu, J.C. *Forensic Accountants' Strategies and Cybercrime Mitigation*; Northcentral University: Scottsdale, AZ, USA, 2020.
9. Momoh, I.; Adelaja, G.; Ejiwumi, G. *Analysis of the Human Factor in Cybersecurity: Identifying and Preventing Social Engineering Attacks in Financial Institution*; IEEE: Piscataway, NJ, USA, 2023.
10. Wendt, D.W. *Exploring the Strategies Cybersecurity Specialists Need to Improve Adaptive Cyber Defenses within the Financial Sector: An Exploratory Study*; Colorado Technical University: Colorado Springs, CO, USA, 2020.
11. Jasper, S. *Strategic Cyber Deterrence: The Active Cyber Defense Option*; Rowman & Littlefield: Lanham, MD, USA, 2017.
12. Angafor, G.N.; Yevseyeva, I.; He, Y. Game-based learning: A review of tabletop exercises for cybersecurity incident response training. *Secur. Priv.* **2020**, *3*, e126. [CrossRef]
13. Franke, U.; Brynielsson, J. Cyber situational awareness—A systematic review of the literature. *Comput. Secur.* **2014**, *46*, 18–31. [CrossRef]
14. Haney, J.; Lutters, W. Security awareness training for the workforce: Moving beyond "check-the-box" compliance. *Computer* **2020**, *53*, 91–95. [CrossRef]
15. Wash, R.; Rader, E. Too much knowledge? security beliefs and protective behaviors among united states internet users. In *Eleventh Symposium on Usable Privacy and Security (SOUPS 2015)*; Michigan State University: East Lansing, MI, USA, 2015.
16. Wash, R. Folk models of home computer security. In Proceedings of the Sixth Symposium on Usable Privacy and Security, Redmond, WA, USA, 14–16 July 2010.
17. Camp, L.J. Mental models of privacy and security. *IEEE Technol. Soc. Mag.* **2009**, *28*, 37–46. [CrossRef]
18. Grinter, R.E.; Edwards, W.K.; Newman, M.W.; Ducheneaut, N. The work to make a home network work. in ECSCW 2005. In Proceedings of the Ninth European Conference on Computer-Supported Cooperative Work, Paris, France, 18–22 September 2005.
19. Bada, M.; Sasse, A.M.; Nurse, J.R. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv* **2019**, arXiv:1901.02672.
20. Furnell, S.; Vasileiou, I. Security education and awareness: Just let them burn? *Netw. Secur.* **2017**, *2017*, 5–9. [CrossRef]
21. Katsikas, S.K. Health care management and information systems security: Awareness, training or education? *Int. J. Med. Inform.* **2000**, *60*, 129–135. [CrossRef] [PubMed]
22. ENISA. The New Users' Guide: How to Raise Information Security Awareness. 2008. Available online: https://www.europeansources.info/record/the-new-users-guide-how-to-raise-information-security-awareness/ (accessed on 1 August 2024).
23. de Zafra, D.E.; Pitcher, S.I.; Tressler, J.D.; Ippolito, J.B. Information technology security training requirements: A role-and performance-based model. *NIST Spec. Publ.* **1998**, *800*, 800–816.
24. Chaudhary, S.; Gkioulos, V.; Katsikas, S. Developing metrics to assess the effectiveness of cybersecurity awareness program. *J. Cybersecur.* **2022**, *8*, tyac006. [CrossRef]
25. Kruger, H.A.; Kearney, W.D. A prototype for assessing information security awareness. *Comput. Secur.* **2006**, *25*, 289–296. [CrossRef]
26. Fan, J.; Zhang, P. Study on e-government information misuse based on General Deterrence Theory. In Proceedings of the ICSSSM11, Tianjin, China, 22–27 June 2011.
27. Ng, B.-Y.; Kankanhalli, A.; Xu, Y. Studying users' computer security behavior: A health belief perspective. *Decis. Support Syst.* **2009**, *46*, 815–825. [CrossRef]
28. Sabillon, R. The cybersecurity awareness training model (CATRAM). In *Research Anthology on Advancements in Cybersecurity Education*; IGI Global: Hershey, PA, USA, 2022; pp. 501–520.
29. Longo, G.; Orlich, A.; Musante, S.; Merlo, A.; Russo, E. MaCySTe: A virtual testbed for maritime cybersecurity. *SoftwareX* **2023**, *23*, 101426. [CrossRef]
30. Li, J.; Li, J.; Xie, C.; Liang, Y.; Qu, K.; Cheng, L.; Zhao, Z. PipCKG-BS: A Method to Build Cybersecurity Knowledge Graph for Blockchain Systems via the Pipeline Approach. *J. Circuits Syst. Comput.* **2023**, *32*, 2350274. [CrossRef]
31. Lee, C.; Lee, S. Evaluating the Vulnerability of YOLOv5 to Adversarial Attacks for Enhanced Cybersecurity in MASS. *J. Mar. Sci. Eng.* **2023**, *11*, 947. [CrossRef]
32. Löffler, E.; Schneider, B.; Zanwar, T.; Asprion, P.M. CySecEscape 2.0-A virtual escape room to raise cybersecurity awareness. *Int. J. Serious Games* **2021**, *8*, 59–70. [CrossRef]

33. Tai, Y.; Wei, L.; Zhou, H.; Peng, J.; Li, Q.; Li, F.; Zhang, J.; Shi, J. Augmented-reality-driven medical simulation platform for percutaneous nephrolithotomy with cybersecurity awareness. *Int. J. Distrib. Sens. Netw.* **2019**, *15*, 1550147719840173. [CrossRef]
34. Hodhod, R.; Hardage, H.; Abbas, S.; Aldakheel, E.A. CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. *Electronics* **2023**, *12*, 3544. [CrossRef]
35. Sharif, K.H.; Ameen, S.Y. A Intelligent Security Power Lab (SPL): The Ultimate Serious Game Training in Cybersecurity. *Int. J. Intell. Syst. Appl. Eng.* **2023**, *11*, 245–259.
36. Wang, P.; Liu, J.; Zhong, X.; Zhou, S. A Cybersecurity Knowledge Graph Completion Method for Penetration Testing. *Electronics* **2023**, *12*, 1837. [CrossRef]
37. Tran, T.M.; Beuran, R.; Hasegawa, S. Gamification-Based Cybersecurity Awareness Course for Self-regulated Learning. *Int. J. Inf. Educ. Technol.* **2023**, *13*, 724–730. [CrossRef]
38. Douha, N.Y.-R.; Sasabe, M.; Taenaka, Y.; Kadobayashi, Y. An Evolutionary Game Theoretic Analysis of Cybersecurity Investment Strategies for Smart-Home Users against Cyberattacks. *Appl. Sci.* **2023**, *13*, 4645. [CrossRef]
39. Ortiz-Garces, I.; Gutierrez, R.; Guerra, D.; Sanchez-Viteri, S.; Villegas-Ch, W. Development of a Platform for Learning Cybersecurity Using Capturing the Flag Competitions. *Electronics* **2023**, *12*, 1753. [CrossRef]
40. Hijji, M.; Alam, G. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors* **2022**, *22*, 8663. [CrossRef] [PubMed]
41. Puys, M.; Thevenon, P.H.; Mocanu, S.; Gallissot, M.; Sivelle, C. SCADA Cybersecurity Awareness and Teaching with Hardware-In-The-Loop Platforms. *J. Wirel. Mob. Netw. Ubiquitous Comput. Dependable Appl.* **2022**, *13*, 4–32.
42. Abu-Amara, F.; Almansoori, R.; Alharbi, S.; Alharbi, M.; Alshehhi, A. A novel SETA-based gamification framework to raise cybersecurity awareness. *Int. J. Inf. Technol.* **2021**, *13*, 2371–2380. [CrossRef]
43. Khader, M.; Karam, M.; Fares, H. Cybersecurity awareness framework for academia. *Information* **2021**, *12*, 417. [CrossRef]
44. Back, S.; Guerette, R.T. Cyber Place Management and Crime Prevention: The Effectiveness of Cybersecurity Awareness Training Against Phishing Attacks. *J. Contemp. Crim. Justice* **2021**, *37*, 427–451. [CrossRef]
45. Nikoloudakis, Y.; Kefaloukos, I.; Klados, S.; Panagiotakis, S.; Pallis, E.; Skianis, C.; Markakis, E.K. Towards a machine learning based situational awareness framework for cybersecurity: An SDN implementation. *Sensors* **2021**, *21*, 4939. [CrossRef]
46. Alves, F.; Bettini, A.; Ferreira, P.M.; Bessani, A. Processing tweets for cybersecurity threat awareness. *Inf. Syst.* **2020**, *95*, 101586. [CrossRef]
47. Gasiba, T.E.; Lechner, U.; Pinto-Albuquerque, M. Sifu—A cybersecurity awareness platform with challenge assessment and intelligent coach. *Cybersecurity* **2020**, *3*, 24. [CrossRef]
48. Alqahtani, H.; Kavakli-Thorne, M. Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). *Information* **2020**, *11*, 121. [CrossRef]
49. Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A.; Bukauskas, A. Juozapavičius, A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Secur.* **2020**, *88*, 101607. [CrossRef]
50. Beuran, R.; Tang, D.; Tan, Z.; Hasegawa, S.; Tan, Y.; Shinoda, Y. Supporting cybersecurity education and training via LMS integration: CyLMS. *Educ. Inf. Technol.* **2019**, *24*, 3619–3643. [CrossRef]
51. Giannakas, F.; Papasalouros, A.; Kambourakis, G.; Gritzalis, S. A comprehensive cybersecurity learning platform for elementary education. *Inf. Secur. J. Glob. Perspect.* **2019**, *28*, 81–106. [CrossRef]
52. Sabillon, R.; Serra-Ruiz, J.; Cavaller, V. An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness Training Model (CATRAM). A case study in Canada. *J. Cases Inf. Technol.* **2019**, *21*, 26–39. [CrossRef]
53. Zhang, Z.; He, W.; Li, W.; Abdous, M. Cybersecurity awareness training programs: A cost–benefit analysis framework. *Ind. Manag. Data Syst.* **2021**, *121*, 613–636. [CrossRef]
54. Fatokun, F.; Awang, Z.; Hamid, S.; Fatokun, J.O.; Norman, A. Cybersecurity Knowledge Deterioration and the role of Gamification Intervention. *J. Adv. Res. Appl. Sci. Eng. Technol.* **2024**, *43*, 66–94. [CrossRef]
55. Tay, A.; Hayes, S.M.; Wilson, D.; Hall, E.; Kaufman, D. Gamified Cybersecurity Education Through the Lens of the Information Search Process: An Exploratory Study of Capture-the-Flag Competitions [Research-in-Progress]. *Issues Informing Sci. Inf. Technol.* **2024**, *21*, 001. [CrossRef]
56. Bandeira, M.; Vairinhos, M.; Dias, P.; Soengas, R.; Silva, V. ChemXP AR Edition, a Serious Game. In *Videogame Sciences and Arts*; Springer Nature: Cham, Switzerland, 2024.
57. Kalmpourtzis, G. *Educational Game Design Fundamentals: A Journey to Creating Intrinsically Motivating Learning Experiences*; AK Peters/CRC Press: Natick, MA, USA, 2018.
58. Stylianidou, N.; Sofianidis, A.; Manoli, E.; Meletiou-Mavrotheris, M. "Helping Nemo!"—Using augmented reality and alternate reality games in the context of universal design for learning. *Educ. Sci.* **2020**, *10*, 95. [CrossRef]
59. Katsantonis, M.N.; Manikas, A.; Mavridis, I.; Fouliras, P. tCOFELET: Conceptual Framework for Team-Centric e-Learning and Training. *IEEE Access* **2024**, *12*, 78878–78894. [CrossRef]
60. Yadav, P. *Gamification and Personalised Learning: Enhancing Student Engagement in Higher Education, in Transforming Education for Personalized Learning*; IGI Global: Hershey, PA, USA, 2024; pp. 85–99.
61. Wang, S.; Kong, X.; Wang, N. Gamification for Learning: Development and Application of Learning Software for Enhancing Student Engagement and Motivation. In Proceedings of the 2024 13th International Conference on Educational and Information Technology (ICEIT), Chengdu, China, 22–24 March 2024.

62. Rosedi, S.R.b.H.M. The Use of Gamification in Improving Student Engagement When Learning the Standard Marine Communication Phrases (SMCP). *KMI Int. J. Marit. Aff. Fish.* **2024**, *16*, 1–20. [CrossRef]
63. Cortes, A.A. Gamifing the Classroom: Bringing Videogames to Life Through Innovation in Education to Increase Student Engagement in STEM Subjects. In Proceedings of the 2024 IEEE Gaming, Entertainment, and Media Conference (GEM), Turin, Italy, 5–7 June 2024.
64. Faith, B.F.; Long, Z.A.; Hamid, S. Promoting cybersecurity knowledge via gamification: An innovative intervention design. In Proceedings of the 2024 Third International Conference on Distributed Computing and High Performance Computing (DCHPC), Tehran, Iran, 14–15 May 2024.
65. Zhang, W.; Wang, M.; Han, G.; Feng, Y.; Tan, X. A Knowledge Graph Completion Algorithm Based on the Fusion of Neighborhood Features and vBiLSTM Encoding for Network Security. *Electronics* **2024**, *13*, 1661. [CrossRef]
66. Barron, R.; Eren, M.E.; Bhattarai, M.; Wanna, S.; Solovyev, N.; Rasmussen, K.; Alexandrov, B.S.; Nicholas, C.; Matuszek, C. Cyber-Security Knowledge Graph Generation by Hierarchical Nonnegative Matrix Factorization. In Proceedings of the 2024 12th International Symposium on Digital Forensics and Security (ISDFS), San Antonio, TX, USA, 29–30 April 2024.
67. Serles, U.; Kärle, E.; Hunkel, R.; Fensel, D. German Tourism Knowledge Graph. *arXiv* **2024**, arXiv:2404.09587.
68. Shi, Z.; Matyunin, N.; Graffi, K.; Starobinski, D. Uncovering CWE-CVE-CPE Relations with threat knowledge graphs. *ACM Trans. Priv. Secur.* **2024**, *27*, 1–26. [CrossRef]
69. Nelson, C.; Shoshitaishvili, Y. PWN The Learning Curve: Education-First CTF Challenges. In Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1, Portland, OR, USA, 20–23 March 2024.
70. Érsok, M.; Erdődi, L.; Balogh, Á.; Bánáti, A. Improving CTF Event Organization: A Case Study on Utilizing Open Source Technologies. In Proceedings of the 2024 IEEE 22nd World Symposium on Applied Machine Intelligence and Informatics (SAMI), Stará Lesná, Slovakia, 25–27 January 2024.
71. Karampidis, K.; Panagiotakis, S.; Vasilakis, M.; Lamari, A.T.; Markakis, E.; Papadourakis, G. Digital Training for Cybersecurity in Industrial Fields via virtual labs and Capture-The-Flag challenges. In Proceedings of the 2023 32nd Annual Conference of the European Association for Education in Electrical and Information Engineering (EAEEIE), Eindhoven, The Netherlands, 14–16 June 2023.
72. Savin, G.M.; Asseri, A.; Dykstra, J.; Goohs, J.; Melaragno, A.; Casey, W. Battle ground: Data collection and labeling of ctf games to understand human cyber operators. In Proceedings of the 16th Cyber Security Experimentation and Test Workshop, Marina del ReyMarina del Rey, CA, USA, 7–8 August 2023.
73. Rashkevych, Y.; Semigina, T. Analysis of micro-credentials implementation opportunities in Ukraine and other European countries, International Educational Space. *Educ. Anal. Ukr.* **2024**, *1*, 110–122.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.