SoK: A Proposal for Incorporating Accessible Gamified Cybersecurity Awareness Training Informed by a Systematic Literature Review

Junibel De La Cruz
Aerstone Cybersecurity
InSPIRIT Lab - University of Denver
junibel.delacruz@aerstone.com

Sanchari Das
InSPIRIT Lab
University of Denver
Sanchari.Das@du.edu

***Abstract*—Gamification is an interactive technology that enhances the user experience by designing modular objectives into game-design elements. In the same manner, gamification has the potential to enhance cybersecurity Awareness for neurodiverse individuals and people with disabilities by using Assistive Technology (AT) to achieve reward-system objectives. To understand further, we conducted a detailed systematization of knowledge (SoK) on 71 peer-reviewed publications concentrating research efforts to increase cybersecurity awareness through accessible gamification. The findings of this SoK establish fundamental components required to address the inclusive nature of gamification in cybersecurity and thereby identify requirements gathering objectives for impacting increased results in raising cybersecurity awareness. After a methodical process of iterative screening and manual analysis in this targeted subject matter, we found that only 9 out of the 71 gamified cybersecurity research initiatives directly address "accessibility" and the implementation methods for game-design elements that would facilitate accessible user-experience. Moreover, a cross-functional Learning Management System (LMS) and Modular Reward System can be optimized by data formulated through a Technology Acceptance Model (TAM) for people with disabilities using AT. Lastly, we propose that a modular training format should effectively engage and facilitate user interface and user experience despite context-oriented limitations on physical.**

I. Introduction

A security learning initiative for cybersecurity education is proposed by addressing inclusive cybersecurity awareness and training. In this regard, cybersecurity awareness can be contextualized as the ability to recognize vulnerable network or technology-based scenarios in the matter of unsecured forms of internet usage and security-related controls [90]. Awareness methods, on the other hand, can be implemented in areas of cybersecurity by applying security principles to daily personal-use activities such as flagging phishing emails, restricting access to unknown wifi networks, password managing, and avoiding cyber-criminal activities [3]. To enhance cybersecurity awareness for daily users to practice indefinitely, gamified methods of training and enhancement can present an enhanced cognitive approach for the increased recognition of cybersecurity education and application [68]. Although basic cybersecurity hygiene is widely induced, whether by compliance or on-premise demand, an inclusive and accessible approach will be even more significant for internet technology users that may have disabilities or neurodiverse learning capacities [42].

Furthermore, considering a vulnerable population for cybersecurity special education will bridge the gap in areas of learned technical usability and cybersecurity application that may be limited in scope for accessible UX requirements via industry and academia training forums [80]. For vulnerable populations and less technical internet users, the challenge of recognizing and practicing secure online activity is limited to the training resources and educational systems available [31]. More importantly, a post-covid learning environment emphasizes accessibility requirements needed to be addressed and optimized for a more productive and secure educational environment at home [35].

Research initiatives for advancing socio-technical interoperation of cybersecurity training should stress inclusive design strategies that directly ensure people with disabilities and neurodiversity have equal opportunity for participation in gamified events. As a resolve, Inclusive Gamified Cybersecurity Awareness facilitates end-user education and assists users to become more resilient to cyber threats. Along these lines, designing an advanced gamified learning management system (LMS) to enhance cybersecurity awareness for an inclusive audience creates user-engagement activities directly impacting motivation for Cybersecurity professional development and security awareness practices and participation [17]. Indeed, the power of gamification enhances learning outcomes and improves access to individuals with auditory, cognitive, neurological, physical, speech, or visual disabilities [38]. Therefore the gamification of educational curricula for disabled learners should integrate accessible instructional designs defining the game elements to motivate users to progress considerably in a gamified cybersecurity environment [25].

Cybersecurity gamification itself has substantially progressed in training aspects, particularly in a team environment. Buchler [11] states that "Cyber competitions offer an approach to train and evaluate the performance of cyber defense teams; such competitions are now regularly conducted at the

Usable Security and Privacy (USEC) Symposium 2022
28 April 2022, San Diego, CA, USA
ISBN 1-891562-79-7
https://dx.doi.org/10.14722/usec.2022.23080
www.ndss-symposium.org, https://www.usablesecurity.net/USEC/

high school, college, professional, and military defense levels. These naturalistic exercises of teamwork for cyber defense represent an important source for understanding the way defense teams form, coordinate, and organize. The gamified cyber exercises also help to determine the factors that make teams more or less successful." Exceptional methods tested in Buchler's [11] study for sociometric, observational assessment of teaming, and leadership in a cybersecurity defense competition demonstrate the implemented use of a 16-point teamwork instrument called OAT (Observational Assessment of Teamwork) to assess teamwork and leadership behaviors in cyber defense. An inclusive multi-player Cyber game LMS may require the OAT framework to record user participation and assessment data of enhanced awareness per training module designed with accessibility [39]. Integrating an OAT teamwork instrument as a component of the game-element structure serves as a cross-functional feature that inclusive cyber games can successfully achieve in this proposal. Therefore, game designers may consider facilitating a socio-technical approach by defining LMS components addressing inclusive requirements for neurodiverse individuals. Thus, strengthening users' social communication strategies in a team environment.

In the same manner, inclusive gamified cybersecurity should require an advanced special education LMS that can evaluate and identify user-interface deficiencies in limited accessibility-based virtual learning platforms [14]. To specialize in technological instruction for people with disabilities, a further scope is narrowed down to determine the best pathway for security training in a modular approach that can be gamified, accessible, and advanced in design utilizing research-proven frameworks that require further operational development [57], [75].

To understand further the concept, we conducted this Systematization of Knowledge (SoK), a comprehensive analysis of publications and user studies to analyze the inclusiveness of research-driven cybersecurity games. The analysis on 71 collected publications discusses the effective measures required for game-design elements that will fill in the research gaps found in user-interface accessibility for our proposed modular approach in security game training. This SoK, therefore, classifies schemes of knowledge from multidisciplinary research across domains in cybersecurity awareness gamification, and Accessible/Inclusive requirements gathering for the neurodiverse and disabled population [29]. The aim of these findings will be used to inform modular game development that shall incorporate advanced LMS functionality to address neurodiversity, training accessibility, and serious game elements in the realm of cybersecurity. Baseline considerations for developing modular game elements will consider zero technical skill level and AT methods of accessibility.

The methodical approach of categorizing domain knowledge in gamified cybersecurity also delimits sub-research domains specifically for end-users with learning disabilities. To do so, an initial classification by relevance was categorized from search terms across multiple databases to extract titles and abstracts. The procedural steps for conducting this systematization of knowledge were ordered according to standards for initializing search strategies and managing data collection records [52]. A detailed analysis was conducted using both automated tools and a manual review of bibliographies, titles, abstracts, and full-text screening for the consolidated sample set collected. The results of 71 analyzed papers indicate most relevant developing subjects focused particularly on gamification for cybersecurity.

II. Background Literature

The background review covers cross disciplines in gamification, special education, learning enhancements, and inclusive security training. The breadth of principles and guidelines in these domains motivate the approach of informing a thematic analysis in later methods of classifying research findings of this SoK.

A. The Role of Gamification

The role of gamification in a software integrated world presents innovative mechanisms to invite users of all ages and backgrounds to engage in serious game training [2]. Research shows the incentives of a gamified reward system increase participants' productivity [34]. Furthermore, the elements of a game design can serve as essential building blocks to develop users' cognitive performance for educational purposes [35]. For example, researchers Huotari and Hamari discuss how gamification can be treated as a service that enhances the objectives of gamified rules in order to achieve optimized experiences with knowledgeable systematic understanding [36]. In like manner, Deterding et al. [24] discuss game-design elements as "gamefulness:" defining gamification as a means of enriching products, services, and information systems with game-design elements in order to positively influence motivation, productivity, and behavior of users. The design of game elements with a systemic understanding of user engagement enables participants to gain aptitude per interactive session in a progressive way. Additionally, Blohm writes in gamification research on, "Gamification: Design of IT-Based Enhancing Services for Motivational Support and Behavioral Change." [10]. Blohm's findings conclude that the benefits of gamification result in the increase of user satisfaction: The continuous documentation of one's own behavior visualizes progress, facilitates the derivation of achievable personal goals, and offers immediate feedback so that users perceive feelings of high individual performance. [10]

Further motivation for game-design elements may enhance user engagement by featuring multi-player modals [65]. Because of limited accessibility in computer science education for a neurodiverse population, an individualized special education system is usually required in order to increase accessibility for learning the fundamentals of cybersecurity [60]. However, an inclusive cybersecurity game can unify neurodiverse trainees to participate with peers, while engaging in enhanced security training in a multi-player context [61]. Engagement across all fronts of gamified serious game training should consider methods for increasing cybersecurity awareness in underserved population groups, such as disabled and neurodiverse communities.

Programs taking a stand for accessible educational initiatives of neurodiverse individuals include the Disability Access Route to Education (DARE) program. DARE reports an urgent emphasis for AT integrated virtual platforms as well as the use-case of advanced learning support systems in high priority

to equip neurodiverse students with more educational opportunities in STEAM subjects [6], [35], [67], [19]. By way of illustration, initiatives such as DARE may consider cooperation to create educational opportunities for students to engage in jeopardy style CTF modules designed for students with zero technical knowledge [50]. The integration of research methods in AT LMS, and cyber education must cross collaborate with a matrix of community requirements for socio-technical accessibility in education, industry, and nonprofits alike. Just as CTF events have had a major impact in cross-cultural contexts for increased levels of novice participation, a call for active engagement in inclusive CTF novice training should be coordinated in equal respects. The research identified in this systematic review collected a series of CTF use-cases that address audiences with zero-to-limited technical capacity. Nevertheless, the zero-to-limited users didn't necessarily imply that the novice CTF events were considered completely accessible to neurodiverse or disabled users.

For instance, a cybersecurity game called PicoCTF was developed for middle to high school students with zero technical security knowledge. PicoCTF acted as capture the flag computer security exercise layered on video game-design elements that trained students in obtaining technical skills, such as reverse engineering, forensics, cryptography, and binary exploitation [59]. The developers of PicoCTF actually emphasized the need to increase accessibility and maintain inclusiveness in their statements of research limitations and future work. As a result, this SoK addresses the inclusive requirements needed to implement AT and advanced LMS inter-operable with effective baseline educational cybersecurity games, such as PicoCTF [86].

Accessing cybersecurity training is essential for enhancing awareness of best security practices for personal and professional purposes. Therefore, providing an innovative gamified training platform considering an inclusive audience becomes even more pragmatic in order to assess how gamification can be a revelation for users' cybersecurity awareness [48]. Prior research in gamified user studies finds that cybersecurity gamification, in regards to realistic game design and the contextualization of the game, does have a notable influence on user engagement [85]. Game-design aspects and game-context serve as examples of best practices in game development and a means to evaluate the learning effectiveness of the game [80]. The results suggest a high correlation between playing the game and succeeding in cybersecurity awareness training [8], [66]. While analyzing students' perceptions, research indicates that the gamification of cybersecurity enables students to therefore increase awareness. To incorporate features of virtualization and visual design of Capture the Flag (CTF) competitions, accessibility components are taken into high consideration for future work of user-interface enhancements in the deployment of inclusive game-design mechanisms and exercises for modular objectives per challenge in a given CTF exercise [18], [73], [78].

With these research objectives in mind, serious-game training in cybersecurity education can advance inclusive audiences through gamification and therefore enable the disabled end-users to enhance their cybersecurity awareness [66]. Fundamentally, we find that gamifying awareness in cybersecurity training engages users to optimize productivity levels with enhanced user-experience features that play into building confidence and skill level through modular reward systems [31]. Further, increasing user participation in gamified cybersecurity awareness also improves disability management and accessibility by intentionally enhancing the user experience for educational purposes [77].

For instance, gamification researchers on cybersecurity education strategy found that students with active learning skills can enforce cybersecurity concepts by measuring performance in a gamified experience [28], [44], [47], [48], [69]. In their work, Malone et al. discuss gamified objectives for increasing cybersecurity awareness through the means of assessing user learning skills in applied curriculum rubrics [48]. Moreover, educational approaches to gamification present innovative methods for enhancing user experience and awareness by ensuring accessibility in gamified frameworks for people with disabilities [1]. Therefore, increasing user engagement with features such as reward systems in Capture the Flag (CTF) style modules demonstrate a successful learning outcome lining up with computer security educational objectives [5], [15], [37], [64], [84].

B. Gamification for Disabled Community

It is imperative that special education systems evaluate the research gaps that people with disabilities face in accessing technological instruction [14], [75]. As mentioned before, the DARE program advocates for AT requirements and advanced learning support systems that will help equip disabled students with educational opportunities in STEAM subjects [6], [67]. Ideally, an inclusive cybersecurity game design may implement supportive tools for special education in computer science that will engage users in various forms of participation as part of an accessible user-experience design. For example, this literature review identifies a key research case study operating with Assistive Technology (AT) that uses Machine Learning and Image Processing techniques to improve user learning in a special education context. A desktop gamification supportive tool called ATHWELA, demonstrates how researchers successfully implement AT software in conjunction with computer science learning exercises, thus finding an increase in user performance that maintains significant approval for functional capabilities of individuals with disabilities [54]. Utilizing AT software via API or software integration design can benefit inclusive cybersecurity serious-game training by actively addressing LMS operational progress in user activity [7]. For example, the use of a CTF gamified format in conjunction with AT software can enhance a modular reward system and increase user participation and training development respectively [68], [81].

Zahid et al. use the Technology Acceptance Model (TAM) to understand the outcome and impact of ICT interventions for disabled people in a use-case study conducted in Bangladesh, (examining end-user demographics and sociometric to evaluate disabled population sample of responses) [88]. In accordance with TAM, the use and benefits of a system rely heavily on the motivation of the actual user, which is influenced by external factors and tangible capabilities of a system [88]. TAM research findings imply that inclusive gamified platform should require enabling user-experience features so that disabled end-users may enhance cybersecurity their awareness

in this proposed modular approach to accessible serious-game design [13], [30], [32], [43]. To further analyze UX research in this modular proposal, inclusive assessments of user-perception for people with disabilities in gamified cybersecurity awareness are increasingly significant for designing formative accessible game-design elements.

C. Cybersecurity Component

In a panel on the Humans and Technology for Inclusive Privacy and Security, authors state that "In the privacy and security research domain, underserved populations may include persons with disabilities, children, older adults, and people from non-Western developing countries. As a result, we often find non-inclusive designs in the privacy and security domain due to many biased assumptions. These inappropriate assumptions could lead to significant challenges for under-served users to utilize privacy mechanisms" [20], [72]. The result of this systematic review underscores the need for user perception designs mindfulness of people with disabilities in the realm of gamified cybersecurity [40]. To facilitate digital inclusion for people with disabilities, the Technology Acceptance Model (TAM) is implemented based on the Theory of Reasoned Action (TRA) [27]. TAM and TRA propose indispensable principles for optimizing user acceptance and usage behavior of information technology [23].

Through this research, our goal is to understand the gamification impact of cybersecurity awareness, especially for the disabled community. To do this, we followed the study architecture of a systematic literature review. The reason is, systematic literature reviews assist in a comprehensive analysis of prior research studies so that results may provide consolidated information on which aspect of research to develop. The methodological approach notes that a systematic literature review or systematization of knowledge research establishes a holistic overview and a basis for the research undertaken. Such analysis helps to direct future work in respective fields and find areas of further research and development [45]. The SoK aims to integrate objectively and systematic results of empirical data collected based on a particular research topic to determine the state of the question in its field of study [26]. Our systematic literature review provides an overview of the gamification of cybersecurity awareness research throughout the years. Additionally, we note a dearth of research in the area of the disabled population, thus making this work unique in this field of research.

III. Study Methodology

With our systematic literature review, we focus on the gamification aspect of cybersecurity education. We determine to answer the following Research Questions (RQs):

- *RQ1: What opportunities and resources are available for user awareness of cybersecurity from the gamification lenses of research?*
- *RQ2: How has the gamification of cybersecurity impacted the user perception and knowledge in the realm of cybersecurity awareness, as explored by prior researchers? How are researchers implementing gamification for cybersecurity awareness?*
- *RQ3: What are the major resources in the gamification of cybersecurity research to enable cybersecurity awareness for the disabled population? What are the major needs of the end user's experience in the disabled population for technology accessibility and cybersecurity awareness?*

To comprehensively evaluate the above-mentioned research questions, the detailed systematic review follows the methodologies designed by prior researchers in the field of cybersecurity and privacy [76], [22], [55], [21], [46], [74], [79]. We initiated the process by conducting a keyword-based search in five Digital Libraries (DLs) including IEEExplore, PubHealth, ACM DL, Medline, and Science Direct. The papers were included if: a) those were published in peer-reviewed journals or conferences; b) the papers were full papers and the full-text was either available publicly or through the DLs access portal. If the papers were not available then the respected authors of the publication were contacted; c) those which were written in English. The papers were excluded if: a) the research was presented in a form of posters, work-in-progress, extended abstract, workshop paper; b) if the full text of the published paper was not available; c) if the papers were available in any other language than English. We did not use an open-source translation tool for the data collection. Our method consisted of five steps starting with: keyword-based search, duplicate removal, automated and manual abstract screening, automated and manual full-text screening, and thematic analysis of the collected papers. The overall data collection and screening process has been listed in Figure 1.

A. Data Collection and Screening

1) Keyword-based Search: Data Collection: : As mentioned above, we started by conducting a keyword-based search in the above-mentioned DLs. The data collection process was initialized by a combination of relevant key terms across research areas in the gamification of cybersecurity, as well as end-user access for people with disabilities. The research queries also targeted papers that utilize advanced assistive learning systems to gamify cybersecurity experience. Accordingly, the data collection was based on rules for syntax order and synonymous expressed terms. As a result, a total set of $2,598$ papers was collected. Table I categorizes the distribution of papers based on the keywords across all DLs.

Thereafter, we conducted a duplicate removal procedure, where every duplicate paper was automatically removed by executing a python script that matched titles and page numbers. After applying the duplicate removal, a total of $1,669$ uniquely identified samples of papers were assessed for language limitations. Hence, we only conducted our analysis on papers that were written entirely in English. As a result, given the absence of literary translation for the purposes of this systematic review, a total of $1,542$ publications remained in the data set.

B. Coding and Automated Analysis

1) Automated screening (search terms in $1,542$ *papers):* : Search term algorithms were written in Python to perform automated analysis of key term inquiry-based deduction. For

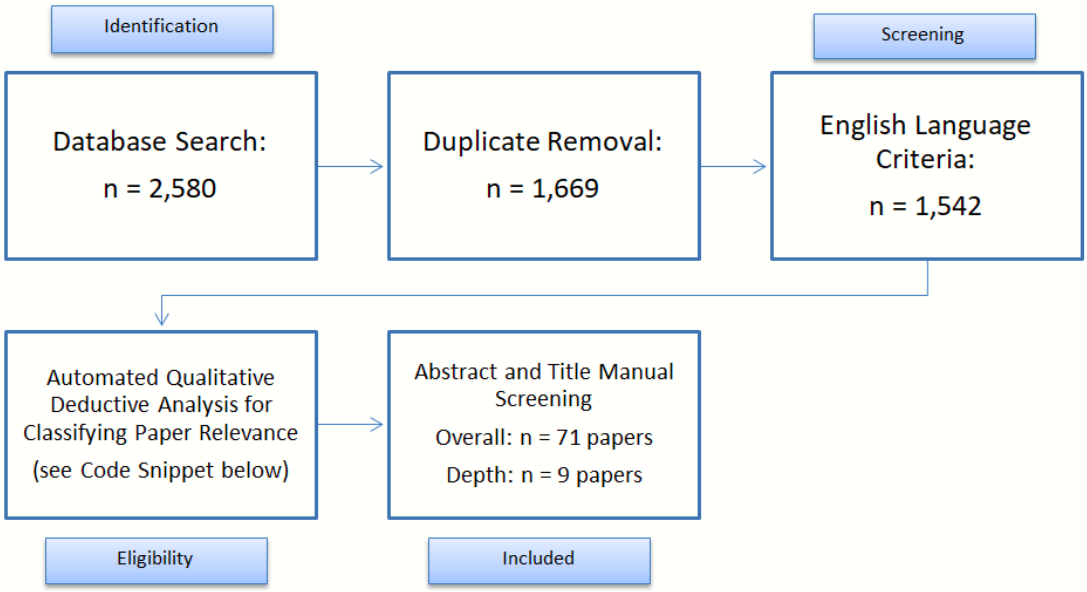

Fig. 1. The Snapshot of the Literature Collection, Screening, and Analysis Utilized in the Systematic Literature Review

TABLE I. THE DISTRIBUTION OF PAPERS IN ALL FIVE DLS BASED ON THE KEYWORD SEARCH USING LOGICAL AND OPERATORS

DL	Results
"Gamified" AND "Cybersecurity"	789
"Gamified" AND "Cybersecurity" AND "Awareness" AND "Disability"	42
"Gamified" AND "Cybersecurity" AND "Awareness"	523
"Gamified" AND "Cybersecurity" AND "Disability"	72
"Gamification" AND "Information Security" AND "Disability"	182
"Gamification" AND "Cybersecurity"	990

example, the scripts addressed the RQs and the search terms were factored into the filtering mechanism to qualify the topic relevance in the titles and abstracts screenings of collected papers sample sets. Subsequently, the automated analysis classified results into multiple subsets and was categorized according to research objectives, therefore evaluating peer-reviewed developments on the gamification of cybersecurity. Moreover, our search term analytics observe keywords relevance to address how the gamification of cybersecurity pertained to the disabled population, as well as overarching themes in the realm of serious games integrated with AT. Ultimately, the automated classification of papers facilitated deductive qualitative analysis to identify common themes across the papers. The first automated screening proceeded with search terms targeting specific areas of research relevant to proposed RQs. Initial rounds of automated analysis exclude irrelevant papers that had no qualitative search criteria in titles and abstract. In the first iteration of the automated analysis. the search term algorithms classified 878 papers by relevance accordingly.

The following automated screening specified quality set terms to identify common themes across data sets focusing on RQs in cybersecurity awareness through gamification, and end-user accessibility for people with disabilities.

```
search_terms= ['cybersecurity awareness',
'CTF accessibility',
'cybersecurity education',
'cybersecurity gamified education',
'cybersecurity training',
'game based cybersecurity',
'gamified skills training',
'gamified cybersecurity',
'cybersecurity serious games',
'gamification cybersecurity education',
'game based training',
'cybersecurity disability management',
'enhancing cybersecurity awareness',
'gamified cybersecurity enhancement',
'gamified technology accessibility',
'disabled gamified user experience',
'disability cybersecurity awareness']
output =
open("output001_from_subset01.csv", 'a')
for line in row:
            if any(word.lower()
            in line.lower()
            for word in searchterms):
                write = csv.writer(output)
                write.writerow(row)
                print(row)
```

To clarify codified objectives, we can see that each recursion of the automated screening derived from the code application contains specific key terms that address RQs proposed. That is to say, the subsets of the outputs from each execution of the algorithm were recursively fed back into new variations of search terms and reiterated the process by re-screening data sets according to keywords specified. In order to further classify results that qualified by relevance for the overview analysis, we were able to arrange research publication to consider for a more thorough analysis.

C. Manual Analysis

As mentioned above, per iteration of our recursive analysis, a manual evaluation of subset outputs applied the following search terms to cross-correlate relevant keywords over titles and abstracts. In brief, each output was manually assessed for eligibility to include in the final dataset.

Code 2: "cybersecurity awareness resources, gamified cybersecurity research, user cybersecurity awareness"

Code 3: "gamification cybersecurity, user perception, cybersecurity awareness"

Code 4: "enabling cybersecurity awareness, disabled population cybersecurity education, accessible end-user experience, assistive technology accessibility, cybersecurity disability management"

Code 5 "information security opportunities, cybersecurity accessible resources, gamified cyber education, gamified security training, research cybersecurity gamification, cybersecurity gamified framework, security game-based design, information security gamified model, awareness training cyber games"

Code 6: "cybersecurity gamification impact, cybersecurity gamified UI, cybersecurity gamified UX, cybersecurity gamified skills training, end-user engagement in gamified cybersecurity"

Code 7: "accessible gamification cybersecurity awareness, disabled population cybersecurity awareness, disability accessibility to cybersecurity resources, enabling the disabled population to increase cybersecurity awareness"

The overall analysis contained 71 papers that had overarching themes distributed across RQs. The depth analysis contained a data set of 9 papers that mentioned some form of accessibility specifically in the context of gamified cybersecurity.

IV. Results

A. Gamified Cybersecurity Awareness Breadth Analysis

1) Thematic Data Extraction: :

A total of five thematic categories were extracted from collected publications in the context of "inclusive gamified cybersecurity apps for neurodiverse individuals." Furthermore, 71 papers are represented in figure 2. Across the manual screening of each paper in the dataset for "accessible cybersecurity games," five categories are systematized in the following order:

1) Gamified Health Apps (addressing some form of end-user accessibility).
2) Assistive Technology (AT), (i.e. Wearables) defining limitations, interoperability, and accessibility requirements, as well as addressing concerns for vulnerable end-user operation of software technology.
3) Training for Assistive Technology (AT) Software for people with disabilities (addressing advanced learning management systems (LMS) that enhance cybersecurity awareness).
4) Cybersecurity Training for neurodiverse individuals (discussing policy issues that limit computer security professional opportunities and restrict cybersecurity awareness).
5) Cybersecurity Healthcare software architecture requirements (researchers developed secure models for vulnerable patients to interface with integrated healthcare technology. In sum, this category observes subthemes in accessibility methods that ensure end-user security and facilitate user experience (UI — UX) in the cybersecurity assisted living context (i.e. IoT Smart Living).

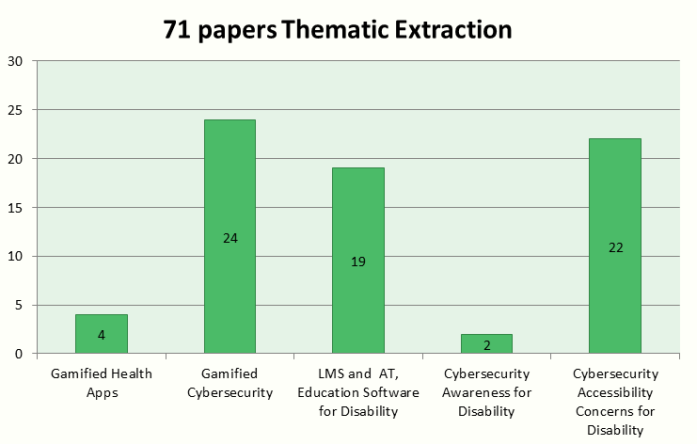

Fig. 2. Distribution of the Extracted Themes from Breadth Analysis delimiting publications addressing Cybersecurity Gamification Awareness in general

The five categories systematized in our breadth analysis evaluate themes of accessible end-user interaction and implementation methods to enhance cybersecurity awareness utilizing end-user operation and technology management. Nonetheless, a subsection of systematized research specifically address gamification of cybersecurity or serious-game training. The systematization of serious-game training is further analyzed in the depth context of end-user eligibility for neurodiversity or disabled parameters.

Accordingly, the overarching themes in the result analysis consist of assistive technology (AT) with subset categories that classify under particular components in RQs, notwithstanding the disregarded keyword selections stated in methodology. As a result of the selection criteria, the manual screening procedure collected the most relevant topics that evaluated specific aspects of gamified technology in a classroom context. A series of search term algorithms were further refined to deduce targeted publications discussing accessible methods and inclusive education for neurodiverse end-users. The result of the thematic extraction resulted in the systematization of gamification healthcare software applications and inclusive serious-game training applications [62], [82], [83], [89]. The subset of publications that were comprehensively considered were systematized in the knowledge domain of gamified cybersecurity enhancement tailoring towards neurodiverse end-users. 9 publications systematized, (12%) discuss awareness training methods to enhance cybersecurity to achieve inclusive gamification.

As referred to in figure 2, the dataset of 71 papers relevant to Cybersecurity UI/UX Disability contained five subcategories

that were manually screened by cross-correlated research domain taxonomy. Equally important, we found that gamified health apps that are designed for end-users with disabilities accounted for only 4 research publications, and 5% research initiatives addressed advanced learning systems (LMS) for UI engagement in training or awareness activities [51], [63], [65], [86]. Furthermore, LMS and AT Educational Software for Neurodiverse end-users count as a subset category for papers matching keyword selection criteria in research domains for learning management systems, AT ecosystem, virtualization, intelligent environments, and analytics focusing on increasing accessibility and secure smart living. In fact, this category accounted for 19 papers, 27% of the dataset in UI/UX research domain [6], [12], [29], [54]. We consolidated the sample set category for Cybersecurity Accessibility Concerns for Neurodiverse individuals to account for 22, 27% of the dataset, where published resources such as a training manual for nurse practitioners, cross-function with cybersecurity awareness, accessibility for neurodiverse individuals and people with disabilities, and smart living technology [33]. The subcategory for Cybersecurity Awareness for Neurodiverse people was addressed in 2 publications, 3% of the papers where awareness and usability were researched and frameworks developed to implement into gamification [60], [70].

The overall analysis of gamified cybersecurity account for 24 publications found, 34% thus addressing gamification education in cybersecurity training informative and evaluative assessments where platforms are developed, deployed, and analyzed [34], [37], [41], [77]. Ultimately, the depth of this systematic literature review seeks to address educational frameworks established specifically for special education end-users in cybersecurity gamification to increase inclusive and accessible cybersecurity awareness.

B. In-Depth Analysis for Accessible Gamification of Cybersecurity for Neurodiverse End-Users

1) Thematic Data Extraction from In-Depth Analysis: : The thematic extraction from our depth analysis shows that 9 research publications from the training framework subset contained related frameworks accessible for gamified cybersecurity educational resources for end-users [12], [13], [48], [49], [66]. In fact, 1 paper out of the 9 mentioned usability of CTF platforms, such as Bin et al. who evaluates the usability of online CTF platforms by implementing a System Usability Scale (SUS) to determine the accessibility of gamified cybersecurity systems [9].

Furthermore, the papers in the systematized depth research analysis category address cybersecurity education for beginners or zero-technical knowledge entry points in games. For example, 2 publications directly emphasize usability and training education made inclusively accessible for people with disabilities [60], [70]. To specify, the paper titled Neurodiverse Knowledge, Skills, and Ability Assessment for CyberSecurity, develops gamified training schemes for neurodiverse individuals (i.e. seeking talent and aptitude from a gamer with autism, ASD) with the NICE framework, thus outlining a set of fundamental cognitive capabilities available to enhance gamified frameworks. Scanlan et al. states that "Serious Games may have a range of benefits for individuals on the autism spectrum over traditional computer-based interventions, since

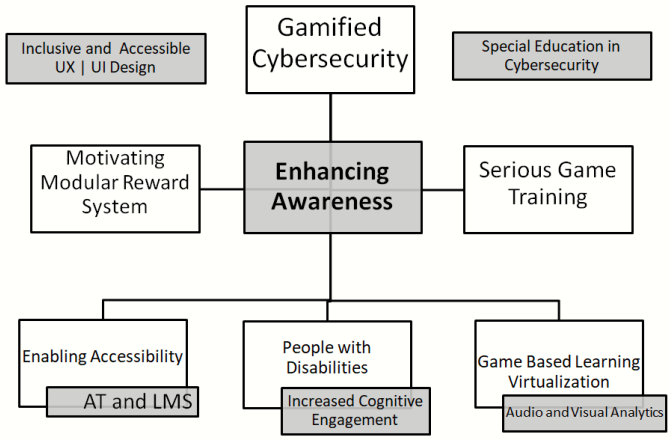

Fig. 3. Thematic Diagram of Gamified Cybersecurity for people with Disabilities

they hold greater potential to enhance skills, including those relating to interpersonal communication [70]."

In comparison with Scalan et al. research findings indicate a virtualized lab environment called Haaukins, which was developed as a completely free and open-source project to boost Cyber Training with unique CTF challenges. Haaukins is a highly accessible and automated virtualization platform for security education, it has three main components (Docker, Virtualbox, and Golang), the communication and orchestration between the components managed using Go programming language. The main reason for having the Go environment manage and deploy something on the Haaukins platform is that Go's easy concurrency and parallelism mechanism [60]. Because accessible gamified cybersecurity software is readily available to users with unique abilities, it is significant to note entry-point requirements for neurodiverse individuals on all technical levels, from beginner to advanced gamified environments.

The thematic diagram of analyzed papers in figure 3, reveals interlocking concepts that are central to the taxonomy of classified and analyzed results. The paper topics systematized highlight key factors associated with the cybersecurity gamification. The majority of the topic comprised of domain knowledge in gamified technical training environments that enhance cybersecurity awareness. For instance, using visual analytics and virtualization with AT elevates player incentives to proceed to the next aligned challenge [13], [48]. In the domain of special education in cybersecurity, the skills enhancement can be programmed in serious game training. The purposes of a rubric lesson objective per module can inform game-design pedagogy using game-based learning [12]. Likewise, using audio and visual analytics to increase cognitive engagement will greatly benefit people with neurodiverse capacities [60]. Furthermore, people with neurodiverse capacities can be enabled with more accessible AT and LMS that will enhance cybersecurity awareness in serious game training [9], [66]. By incorporating a modular reward system, game-design elements assist learning advancement for neurodiverse end-users, by positively impacting the productivity curve due to inclusive and accessible UX — UI Design [70].

	Questions	Highlighted Systematized Key Findings and Details
RQ1	What opportunities and resources are already available for cybersecurity end-user awareness from the gamification lenses of research? How are researchers implementing gamification training in cybersecurity?	Neurodiverse Cybersecurity Abilities Assessments were systematized in results and can be incorporated in requirements gathering for a game-elements modular approach [70], [42]. For example, an inclusive cybersecurity serious game may incorporate an Advanced Multiplayer - SocioMetric Learning Management Systems LMS: 16-point OAT Assessment as proposed by Buchler et al. [11]
RQ2	How has the gamification of cybersecurity impacted the user perception and knowledge in the realm of cybersecurity awareness as explored by prior researchers?	User-studies systematized in the SoK analysis inform accessible requirement gatherings to meet robust ADA compliance innovation, incorporating a Highly accessible platform, and automated virtualization for increased cognitive enhancement security education [62]. SoK analysis considers the Case-by-case Accessibility Requirements Gathering for Neurodiverse end-user as proposed by framework such as in the CTF virtualized open-source framework: Hauukins [60]
RQ3	What are the major resources in the gamification of cybersecurity research to enable cybersecurity awareness for the neurodiverse end-users? What are the major accessibility requirements for end-user's experience in the disabled population for technology accessibility and cybersecurity awareness?	Advanced LMS and AT for inclusive accessibility requirements to be incorporated into cybersecurity serious game-elements should consider modeling approaches to gamified learning, such as Technology Acceptance Model (TAM) Theory of Reasoned Action (TRA) [27], [83], [89] Inclusive ML - AI LMS for Computer Science special education neurodiverse end-users, ATHWELA [54]

TABLE II. ALIGNMENT OF THE RESEARCH QUESTIONS WITH FINDINGS

V. DISCUSSION

Table II discusses the high level overview of the research findings with the RQs. To details, we proposed RQ1: What opportunities and resources are already available for users' awareness of cybersecurity from the gamification lenses of research? How are researchers implementing gamification in cybersecurity? To answer this, we conducted an overall analysis, where we collected and systematized research publications that assessed cybersecurity gamification resources already deployed as open-source projects, such as CTF service engines. Moreover, we found that researchers utilized the CORE framework for gamified cybersecurity as an effective educational method [84].

RQ2 inquires, How has the gamification of cybersecurity impacted user perception and knowledge in the realm of cybersecurity awareness as explored by prior researchers? From the overall analysis, it is worth noting that not all papers that mention accessible platforms for cybersecurity serious games, directly address the implementation and training of neurodiverse end-users to increase cybersecurity awareness. Researchers admit that integrating neurodiverse individuals for instructional need-based game design will always require a different approach based on the case by case special needs [9], [60], [70]. However, we found that researchers developed frameworks to enhance user perception of cybersecurity awareness in gamified strategies. For example, Compte et al. write on A Renewed approach to serious games for cyber security, where a "serious game could potentially reach a larger audience than existing serious games while complying with national cyber strategies. To this end, a framework for designing serious games which are aimed at raising awareness of cybersecurity to those with little or no knowledge of the subject is developed [41]."

Furthermore, 3 publications were systematized by user studies conducted where cybersecurity gamified projects applied advanced LMS to assess participant skills and progress in a capture the flag (CTF) competition [12], [13], [66]. The use of advanced LMS for cybersecurity games such as CTF can be a means for enabling end-user accessibility to increase gamification activity. Therefore, technology accessibility is evaluated in user studies to identify outliers in CTF games. Examining learning outcomes of game-based methods shows the need to design games with constraining efforts. For instance, "If students are given too much freedom, the complex task of creating a cybersecurity game might be daunting. By specifying constraints such as possible topics, network topology, number of levels, and maximum time, we lower the barrier for students to start working on the project. Moreover, having a precise specification of the expected result helps the students deliver results of a higher quality [77]."

Finally, RQ3 inquires "What are the major resources in the gamification of cybersecurity research to enable cybersecurity awareness for the neurodiverse community? What are the major accessibility requirements of end-user experience to enhance cybersecurity awareness?" Panum et al. emphasize accessible CyS "education platform that improves upon this experience, through automation, and individualized learning labs that improve upon typical accessibility issues of students and cumbersome configuration management for organizers (thus platform is named Haaukins) [60]. The virtualization CTF gamification is incorporated in learning labs to enable students with neurodiverse capacities to engage cognitively with higher productivity rates.

Particularly, game-design elements for the gamification of cybersecurity cross-correlated many times with the use of serious games, assistive technology, and cybersecurity awareness resources required for people with disabilities. Hendrix et al. conducted a literature review to examine the effectiveness of games as means of increasing cybersecurity awareness in general [34]. They mention that "Serious Games can be effective tools for public engagement and behavioral change and role play games, are already used by security professionals. Thus cybersecurity seems especially well-suited to Serious Games" [34]. Subsequently, it was found that the game-design elements for serious games and gamified cybersecurity aligned in frequency with CTF competitive sports design. The evaluative assessments conducted in CTF user studies demonstrate the effectiveness of increasing cybersecurity awareness based on the CTF model. For example, WH Tan's Design, motivation, and Framework in game-based learning discuss in chapter 5 the effectiveness of using cybersecurity education framework with CTF design. In the study conducted by Li Jing Khoo, researchers simulate a real-world cyber landscape, with customized cybersecurity CTF games that validate the experiment by observing the relationship between learner motivation and achievement level [16]."

Additionally, the incentives productively increase in gamification activity for neurodiverse end-users, particularly in the development of serious games. Nugent et al. address inclusive gamified cybersecurity assessments in their research, Recruitment AI has a Disability Problem: questions employers should be asking to ensure fairness in recruitment [56]. In like manner, Le et al. review the opportunity landscape neurodiverse end-users limited participation in gamified cybersecurity assessments, stating that "a qualified, visually impaired, cybersecurity expert will only be the best ... when job seekers don't precariously intersect with the computational complexities related to disability, the inherent ... Gamified assessments raise additional concerns related to dexterity, vision impairment, etc [41]." The systematization of these publications discusses major emerging issues and limitations for accessible end-user security across the healthcare IT industry and broad scopes of assistive technology [4], [53], [63].

Provided that privacy and security are evolving into an innovative landscape, the question remains; how are expanding network infrastructures considering our vulnerable population user-experience and accessibility requirements? ADA compliance requires accessible accommodations indeed [71], however with the rapid innovation and disrupted technological workforce, inclusiveness and accessibility become even more imperative, as end-user interface operates and grants us access to our day-to-day interconnected systems and technology. With this in mind, laws and policies regarding sensor network and data management were found prevalent in the effective and secure use of advanced technology for people with disabilities [63]. The rising need for representation in the neurodiverse community demonstrates the need to advocate in public relations for inclusive accessibility rights in technology and cybersecurity computer science education [87]. Understanding the limitations of the accessibility rights can further inform our software designs to intentionally enhance cybersecurity awareness with users' perceptions. The following publication "Externalities and Enterprise Software: Helping and Hindering Legal Compliance," outlines the UNCRPD Digital Accessible Information System Defense Advanced Research Projects Agency and the Disability Discrimination Act, which address work and educational rights for neurodiverse end-users to have increased access and awareness of cybersecurity learning opportunities [58]. Likewise, cybersecurity healthcare architecture systematized research highlights the enabling of socio-technical frameworks for identifying cybersecurity risks to vulnerable end-users [4].

VI. Implications

The results of this (SoK) literature data reveal the indispensable implications required to establish an Inclusive Cybersecurity Professional Development Framework by Raising Cybersecurity Awareness. A Specialized Educational Gamification Format can optimize users' capability to advance cybersecurity objectives interactively with each modular challenge. To demonstrate, the Gamified Framework: "Cyber-Serious Training" is the regarded proposed Creative Curriculum, aligning with CTF (Capture the Flag) principles in advancing user knowledge through a reward point system. The Cyber-Serious Game can be distributed in Mobile Application Format, Web Application Format, and made available via Game Console to increase accessibility across multiple platforms. The interactive online environment will prepare users to completely participate despite the level of technical background, physical limitation, or neurodiversity. The Inclusive Cyber-Serious Game should be formatted to assess and evaluate the users' Challenge Achievement Response Points by incorporating pedagogical metrics and Gamified Cybersecurity Rubric into a built-in Learning Management System (LMS) to monitor Reward Points by observing and analyzing the participants' progress. Furthermore, the Technology Acceptance Model (TAM) [27] should be implemented into the LMS to optimize user acceptance of Cyber-Serious Technology Controls. The Cyber-Serious gamified framework will benefit from user performance by analyzing the impact of modular objectives, users' acceptance of gamified controls, and gamified rubric data displaying an increase in Cybersecurity Awareness and Technical Concepts.

The Cyber-Serious CTF interactive gamification technology shall enhance user motivation and raise Cybersecurity Awareness by modeling CTF concepts and aiding participants' ability to operate gamified software by exercising problem-solving skills. That is to say, the modules serve as a training method to advance user functional skills while solving cybersecurity problems in a CTF format. As a result, the bridge between cyber gamification development and Cyber-Serious CTF is to accessibly modularize Cyber Skills and Concepts mainly addressed to an Inclusive Audience, regardless of neurodiverse learning capacity.

The proposed Cybersecurity Framework: Cyber-Serious (CTF) user-experience research indicates the interactive technology that calls for inclusive accessibility featuring Auditory/Visual/Cognitive enabling accessibility. To ensure a Cyber-Serious (CTF) has usable attributes for an inclusive audience, Cyber-Serious must feature UX qualities including AR, VR, Assistive Technology (AT), Speech-to-Text, Video-Game Tutorial Snippets, Simplified Audio/Video Narration (with T.P.R. or Total Physical Response). To enhance users' learning experience by engaging all technological features, virtual pedagogy, and special education techniques, the designed Cyber-Serious CTF enables and therefore empowers Neurodiverse end-users to enhance Cybersecurity Awareness and participate in advanced technical challenges.

Cyber-Serious (CTF) should also incorporate the gamification Supportive Tool for Special Educational Centers aforementioned, ATHWELA [54] - operating through Assistive Technology. Assistive technology (AT) can be incorporated in the gamification platform as a device or service that increases, maintains, and improves the functional capabilities of individuals with disabilities. Furthermore, the use of AR and VR can be implemented with IT-Based Enhancing Services for Motivational Support and Behavioral Change [10]. Design features and reward systems can respond to LMS rubric completion and display a visualized progress for gamer performance.

To further motivate user engagement and facilitate cybersecurity learning enhancement, the CTF game should incorporate Thematic Components, identifying a player as an individual Avatar and designing creative interactive modules that advance users' professional development potential. The framework should involve a Cybersecurity Work Scenario designed Video-Game to increase Cybersecurity Awareness and Comprehensive Performance. For each CTF module, a

clear objective (FLAG) is set to introduce Cybersecurity key-terms associated with CTF modular activity.

The Skills and Objectives to achieve CTF modules will be initialized by a multi-modal gamified program selection frame, where Modes are either set to MISSION MODE, MULTI-PLAYER MODE, and CAMPAIGN MODE. The Modes will permit users to choose training simulations in 1) MISSION MODE, engage in Cybersecurity Community Events/Conferences/Forums in 2) CAMPAIGN MODE, and engage in 3) MULTI-PLAYER MODE training work scenarios to facilitate collaborative gamified environments. The multi-modal framework allows gamer enhancement and creative approaches to the training curriculum. By designing multiple frames centered around Gamified Cybersecurity, the participants' motivation and technology acceptance increase is likely to correlate with alternative training features.

For all Multi-Modal Programs, an LMS should outline the Gamified Course Progress to achieve the following learning objectives across the course of the gamified program, so that the following Game Levels and Learning Objectives are completed correspondingly. For the MULTI-PLAYER MODE, in the advanced technical challenges game designers can implement Buchler's [11] OAT method to the LMS, for Sociometrics and observational assessment of teaming and leadership in a cyber security competition using a 16-point teamwork instrument called OAT (Observational Assessment of Teamwork) to assess teamwork and leadership behaviors in cyber games.

Key Objectives of the Primary Series of Fundamental Modules Should Require: Defining Cybersecurity Awareness (Key Terms), and establishing Reward Point System for each Challenge-Response Question for the given interactive Key Terms. The module should include Snippet Audio /Video Tutorials that Simplify User's Technical Understanding Required to interact with controls and commands for Gamified Online Technical Environment. After completing Cybersecurity Awareness Vocabulary Training, the user will Capture the Flag, and Advance to the Subsequent Fundamental Module Covering a Range of Topics and Key Terms relevant to the Training Sequence for raising Cybersecurity Awareness. The fundamental training for Inclusive Cyber Serious Games is founded upon the series of the first three modular activities for Mission Mode and Multiplayer Mode. Each Module should require no longer than 15 minutes to complete, while the LMS simultaneously monitors progress and either increases or decreases the complexity of Challenge-Response Actions / Questions for Gamers.

Increasing cybersecurity Awareness through Interactive Vocabulary Training will give users' the comprehensive capability to interact with advanced CTF technical challenges in advanced Modules. Players will be able to apply the mastered vocabulary concepts directly to the technical challenges in cascading modules according to the cybersecurity topic being covered. As a result, the players shall enforce cybersecurity Problem-Solving Skills throughout the modular professional development game. Ultimately, Cyber Serious CTF serves as an Educational Gamified Framework as well as a technical application practice environment to aid all individuals in the advancement and enhancement of Cybersecurity Awareness.

As mentioned in Section II the Disability Access Route to Education (DARE) program called for AT and advanced learning support systems to equip disabled students with educational opportunities in STEAM subjects matters [6], [67]. Taking into account accessible means to design gamified training frameworks will broaden the horizon for students to therefore broaden technical foundation and be actively engaged in advancing their knowledge and awareness in cybersecurity.

VII. Limitations and Future Work

In this research, we conducted a systematic literature review of 71 papers discussing cybersecurity awareness through gamification. Out of the 71 papers, 9 of them discussed the importance of this approach for the disabled community. We have done our due diligence in collecting the papers and conducting the analysis. However, it might be possible we have missed some of the papers. Thus, as an extension of this work, we intend to expand the digital library list to other publication avenues. Additionally, as we found certain gaps in the literature, we plan on creating different gamification modules as mentioned in the implication section catering to the needs and perceptions of the disabled community to enhance their cybersecurity awareness through detailed user studies.

VIII. Conclusion

Evaluation of the prior work collected in this literature review sustains that game-based learning effectively enhances cybersecurity revelation through special education frameworks utilizing end-user design elements. With the presence of assistive technology and learning management systems, instructional elements can therefore be structured in a game design that increases cybersecurity awareness. Similarly, the disabled population can be enabled and enhanced via user experience for gamified cybersecurity awareness activities. Our SoK on peer-reviewed publications analyzed 71 papers and synthesized research domains correlating with cybersecurity awareness through gamification, while particularly concentrating on the disabled community. This SoK identifies thematic elements addressing the inclusive nature of gamification of cybersecurity for people with disabilities and found that 9 of the 71 papers mentioned the need for more accessible educational platforms for inclusive entry-point in cybersecurity games. With this purpose, we conclude the call for cybersecurity awareness games to be made fully accessible to neurodiverse individuals (i.e. ASD) and the disability population, while providing recommendations on the modularized approach. With this in mind, the SoK identifies research gaps for the increased cybersecurity awareness in the disabled community via gamification and provides future directions in this area of research.

IX. Acknowledgement

We would like to acknowledge the Inclusive Security and Privacy-focused Innovative Research in Information Technology (InSPIRIT) Lab at the University of Denver where this research was conducted. Any opinions, findings, conclusions, or recommendations expressed in this material are solely those of the authors.

REFERENCES

[1] J. C. Acosta, J. McKee, A. Fielder, and S. Salamah, "A platform for evaluator-centric cybersecurity training and data acquisition," in *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)*. IEEE, 2017, pp. 394–399.

[2] M. Adams and M. Makramalla, "Cybersecurity skills training: An attacker-centric gamified approach," *Technology Innovation Management Review*, vol. 5, no. 1, 2015.

[3] A. Alzubaidi, "Measuring the level of cyber-security awareness for cybercrime in saudi arabia," *Heliyon*, vol. 7, no. 1, p. e06016, 2021.

[4] K. Anastasopoulou, P. Mari, A. Magkanaraki, E. G. Spanakis, M. Merialdo, V. Sakkalis, and S. Magalini, "Public and private healthcare organisations: a socio-technical model for identifying cybersecurity aspects," in *Proceedings of the 13th International Conference on Theory and Practice of Electronic Governance*, 2020, pp. 168–175.

[5] M. R. Asghar and A. Luxton-Reilly, "Teaching cyber security using competitive software obfuscation and reverse engineering activities," in *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*, 2018, pp. 179–184.

[6] S. Aubakirova, "A comparative analysis of inclusive education systems in ireland and kazakhstan," *Level 3*, vol. 13, no. 1, p. 2, 2016.

[7] O.-G. Baciu-Ureche, C. Sleeman, W. C. Moody, and S. J. Matthews, "The adventures of scriptkitty: Using the raspberry pi to teach adolescents about internet safety," in *Proceedings of the 20th Annual SIG Conference on Information Technology Education*, 2019, pp. 118–123.

[8] R. Beuran, T. Inoue, Y. Tan, and Y. Shinoda, "Realistic cybersecurity training via scenario progression management," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 67–76.

[9] M. H. bin Noor Azam and R. Beuran, "Usability evaluation of open source and online capture the flag platforms," *Japan Advanced Institute of Science and Technology, IS-RR-2018-001: 1-28*, 2018.

[10] I. Blohm and J. M. Leimeister, "Gamification," *Business & information systems engineering*, vol. 5, no. 4, pp. 275–278, 2013.

[11] N. Buchler, P. Rajivan, L. R. Marusich, L. Lightner, and C. Gonzalez, "Sociometrics and observational assessment of teaming and leadership in a cyber security defense competition," *computers & security*, vol. 73, pp. 114–136, 2018.

[12] T. J. Burns, S. C. Rios, T. K. Jordan, Q. Gu, and T. Underwood, "Analysis and exercises for engaging beginners in online {CTF} competitions for security education," in *2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17)*, 2017.

[13] K. Burská, "Visual analytics in cybersecurity education," Ph.D. dissertation, Masaryk University, 2018.

[14] F. Carnide, F. Baptista, S. B. Dias, A. Moura, H. Langberg, A.-M. M. Jensen, and F. Delpozo, "Frailty, falls, and functional loss education: The 3fights@ edu mooc perspective," in *2016 1st International Conference on Technology and Innovation in Sports, Health and Wellbeing (TISHW)*. IEEE, 2016, pp. 1–6.

[15] K. Chain, C.-C. Kuo, I.-H. Liu, J.-S. Li, and C.-S. Yang, "Design and implement of capture the flag based on cloud offense and defense platform," in *2018 IEEE International Conference on Applied System Invention (ICASI)*. IEEE, 2018, pp. 686–689.

[16] R. G. Chicone and S. Ferebee, "A comparison study of two cybersecurity learning systems: Facebook's open source capture the flag and ctfd," *Issues in Information Systems*, vol. 21, no. 1, pp. 202–212, 2020.

[17] N. Chowdhury and V. Gkioulos, "Cyber security training for critical infrastructure protection: A literature review," *Computer Science Review*, vol. 40, p. 100361, 2021.

[18] G. Costa, M. Lualdi, M. Ribaudo, and A. Valenza, "A nerd dogma: Introducing ctf to non-expert audience," in *Proceedings of the 21st Annual Conference on Information Technology Education*, 2020, pp. 413–418.

[19] W. da Silva Guimarães, "Review of serious games for cybersecurity and privacy skills training."

[20] S. Das, R. S. Gutzwiller, R. D. Roscoe, P. Rajivan, Y. Wang, L. Jean Camp, and R. Hoyle, "Humans and technology for inclusive privacy and security," in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, vol. 64. SAGE Publications Sage CA: Los Angeles, CA, 2020, pp. 461–464.

[21] S. Das, A. Kim, Z. Tingle, and C. Nippert-Eng, "All about phishing exploring user research through a systematic literature review," in *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[22] S. Das, B. Wang, Z. Tingle, and L. J. Camp, "Evaluating user perception of multi-factor authentication: A systematic review," in *Proceedings of the Thirteenth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2019)*, 2019.

[23] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," *MIS quarterly*, pp. 319–340, 1989.

[24] S. Deterding, D. Dixon, R. Khaled, and L. Nacke, "From game design elements to gamefulness: defining" gamification"," in *Proceedings of the 15th international academic MindTrek conference: Envisioning future media environments*, 2011, pp. 9–15.

[25] L. Drevin and M. Theocharidou, *Information Security Education. Education in Proactive Information Security: 12th IFIP WG 11.8 World Conference, WISE 12, Lisbon, Portugal, June 25–27, 2019, Proceedings*. Springer, 2019, vol. 557.

[26] T. Ferreras-Fernández, H. Martín-Rodero, F. J. García-Peñalvo, and J. A. Merlo-Vega, "The systematic review of literature in lis: An approach," in *Proceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality*, 2016, pp. 291–296.

[27] M. Fishbein and I. Ajzen, "Belief, attitude, intention, and behavior: An introduction to theory and research," *Philosophy and Rhetoric*, vol. 10, no. 2, 1977.

[28] V. Ford, A. Siraj, A. Haynes, and E. Brown, "Capture the flag unplugged: an offline cyber competition," in *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education*, 2017, pp. 225–230.

[29] M. Fuentes, "Sensor technology, gamification, haptic interfaces in an assistive wearable," in *34th Annual Assistive Technology Conference Scientific/Research Proceedings, San Diego*, 2019.

[30] H. Gonzalez, R. Llamas, and O. M. Rivas, "Using a ctf tournament for reinforcing learned skills in cybersecurity course." *Res. Comput. Sci.*, vol. 148, no. 5, pp. 133–141, 2019.

[31] C. Greenhow, B. Robelia, and J. E. Hughes, "Learning, teaching, and scholarship in a digital age: Web 2.0 and classroom research: What path should we take now?" *Educational researcher*, vol. 38, no. 4, pp. 246–259, 2009.

[32] M. Greenwald, "Cybersecurity in sports," *Questions of Privacy and Ethics. Tufts University Department of Computer Science. Recuperado de http://www. cs. tufts. edu/comp/116/archive/fall2017/mgreenwald. pdf*, 2017.

[33] D. Guzys, R. Brown, E. Halcomb, and D. Whitehead, *An introduction to community and primary health care*. Cambridge University Press, 2020.

[34] M. Hendrix, A. Al-Sherbaz, and B. Victoria, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, 2016.

[35] J. Hernandez, "Teachers' perceptions of integrating digital technology tools," Ph.D. dissertation, Concordia University Chicago, 2021.

[36] K. Huotari and J. Hamari, "Defining gamification: a service marketing perspective," in *Proceeding of the 16th international academic MindTrek conference*, 2012.

[37] S. Karagiannis and E. Magkos, "Engaging students in basic cybersecurity concepts using digital game-based learning: Computer games as virtual learning environments," in *Advances in Core Computer Science-Based Technologies*. Springer, 2021, pp. 55–81.

[38] Z. Khot, K. Quinlan, G. R. Norman, and B. Wainman, "The relative effectiveness of computer-based and traditional resources for education in anatomy," *Anatomical sciences education*, vol. 6, no. 4, pp. 211–215, 2013.

[39] S.-K. Kim, E.-T. Jang, and K.-W. Park, "Toward a fine-grained evaluation of the pwnable ctf," in *International Conference on Information Security Applications*. Springer, 2020, pp. 179–190.

[40] M. Kurosu, *Human-Computer Interaction. Perspectives on Design: Thematic Area, HCI 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, July 26–31, 2019, Proceedings, Part I*. Springer, 2019, vol. 11566.

[41] A. Le Compte, D. Elizondo, and T. Watson, "A renewed approach to serious games for cyber security," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. IEEE, 2015, pp. 203–216.

[42] C. Lesko, "Enabling cybersecurity scholarship: Realizing the requirements for a collaborative multi-functional learning space," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Association for the Advancement of Computing in Education (AACE), 2018, pp. 657–665.

[43] K. Leune and S. J. Petrilli Jr, "Using capture-the-flag to enhance the effectiveness of cybersecurity education," in *Proceedings of the 18th Annual Conference on Information Technology Education*, 2017, pp. 47–52.

[44] C. Li and R. Kulkarni, "Survey of cybersecurity education through gamification," in *2016 ASEE Annual Conference & Exposition*, 2016.

[45] T. Majam and F. Theron, "The purpose and relevance of a scientific literature review: A holistic approach to research," *Journal of public administration*, vol. 41, no. 3, pp. 603–615, 2006.

[46] R. Majumdar and S. Das, "Sok: An evaluation of quantum authentication through systematic literature review," in *Proceedings of the Workshop on Usable Security and Privacy (USEC)*, 2021.

[47] B. Malawski, "Cyber gamification: The use of capture the flag (ctf) and similar exercises to develop critical-thinking and problem-solving skills in cyber graduates," Ph.D. dissertation, Utica College, 2018.

[48] M. Malone, Y. Wang, K. James, M. Anderegg, J. Werner, and F. Monrose, "To gamify or not? on leaderboard effects, student engagement and learning outcomes in a cybersecurity intervention," in *Proceedings of the 52nd ACM Technical Symposium on Computer Science Education*, 2021, pp. 1135–1141.

[49] O. Margalit, "Using computer programming competition for cyber education," in *2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE)*. IEEE, 2016, pp. 104–107.

[50] P. Matias, P. Barbosa, T. N. Cardoso, D. M. Campos, and D. F. Aranha, "Nizkctf: a noninteractive zero-knowledge capture-the-flag platform," *IEEE Security & Privacy*, vol. 16, no. 6, pp. 42–51, 2018.

[51] M. Mettler, "# focusontheenduser: The approach to consumer-centered healthcare," in *Health 4.0: How Virtualization and Big Data are Revolutionizing Healthcare*. Springer, 2017, pp. 109–123.

[52] D. Moher, L. Shamseer, M. Clarke, D. Ghersi, A. Liberati, M. Petticrew, P. Shekelle, and L. A. Stewart, "Preferred reporting items for systematic review and meta-analysis protocols (prisma-p) 2015 statement," *Systematic reviews*, vol. 4, no. 1, 2015.

[53] S. H. Nam, J. Y. Lee, and J. Y. Kim, "Biological-signal-based user-interface system for virtual-reality applications for healthcare," *Journal of Sensors*, vol. 2018, 2018.

[54] P. Nisansala and A. Morawaka, "Athwel: Gamification supportive tool for special educational centers in sri lanka," in *2019 14th Conference on Industrial and Information Systems (ICIIS)*. IEEE, 2019, pp. 446–451.

[55] N. Noah and S. Das, "Exploring evolution of augmented and virtual reality education space in 2020 through systematic literature review," *Computer Animation and Virtual Worlds*, vol. 32, no. 3-4, p. e2020, 2021.

[56] S. Nugent, P. Jackson, S. Scott-Parker, J. Partridge, R. Raper, C. Bakalis, A. Shepherd, A. Mitra, J. Long, K. Maynard *et al.*, "Recruitment ai has a disability problem: questions employers should be asking to ensure fairness in recruitment," *The Institute for Ethical AI*, 2020.

[57] U. S. D. of Labor, "National disability employment awareness month 2021: Native american with disability cybersecurity training, employee of the month, https://www.dol.gov/agencies/odep/initiatives/ndeam," 2021.

[58] T. Otter, *Externalities and Enterprise Software: Helping and Hindering Legal Compliance*. KIT Scientific Publishing, 2019, vol. 18.

[59] K. Owens, A. Fulton, L. Jones, and M. Carlisle, "pico-boo!: How to avoid scaring students away in a ctf competition," *Colloquium for Information Systems Security Education (CISSE)*, 2019.

[60] T. K. Panum, K. Hageman, J. M. Pedersen, and R. R. Hansen, "Haaukins: A highly accessible and automated virtualization platform for security education," in *2019 IEEE 19th International Conference on Advanced Learning Technologies (ICALT)*, vol. 2161. IEEE, 2019, pp. 236–238.

[61] J.-G. Park, S.-H. Choi, H.-i. Kim, and H. Dowon, "Our experiences on the design, build and run of ctf," *The 4th International Conference on Next Generation Computing*, 2018.

[62] S. Philippe, A. D. Souchet, P. Lameras, P. Petridis, J. Caporal, G. Coldeboeuf, and H. Duzan, "Multimodal teaching, learning and training in virtual reality: a review and case study," *Virtual Reality & Intelligent Hardware*, vol. 2, no. 5, pp. 421–442, 2020.

[63] M. Pike, N. M. Mustafa, D. Towey, and V. Brusic, "Sensor networks and data management in healthcare: Emerging technologies and new challenges," in *2019 IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 1. IEEE, 2019, pp. 834–839.

[64] P. Prinetto, G. Roascio, and A. Varriale, "Hardware-based capture-the-flag challenges," in *2020 IEEE East-West Design & Test Symposium (EWDTS)*. IEEE, 2020.

[65] P.-L. P. Rau, *Cross-Cultural Design. Applications in Health, Learning, Communication, and Creativity: 12th International Conference, CCD 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19-24, 2020, Proceedings, Part II*. Springer Nature, 2020, vol. 12193.

[66] S. Ros, S. Gonzalez, A. Robles, L. Tobarra, A. Caminero, and J. Cano, "Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course," *IEEE Access*, vol. 8, pp. 97 718–97 728, 2020.

[67] R. Ryan, "How inequality in education in ireland is produced, reproduced, justified, and resisted at the intersection of disability and social class," Ph.D. dissertation, National University of Ireland, Maynooth (Ireland), 2019.

[68] T. Saldanha, Q. Vinlove, and J. Mache, "Mice: a holistic scorekeeping mechanism for cybersecurity wargames," *Journal of computing sciences in colleges*, vol. 35, no. 1, 2019.

[69] R. E. Santiago Lozada, "Capture the flag (ctf): Website tutorial to boost cybersecurity training," *Computer Science;*, 2019.

[70] J. Scanlan, A. Eddy, T. Thomas, T. Tan, Y.-P. P. Chen, P. A. Watters, M. Fieldhouse, L. Fung, and S. Girdler, "Neurodiverse knowledge, skills and ability assessment for cyber security," *Australasian Conference on Information Systems*, 2020.

[71] A. Scheimann, "Ada compliance: What are we doing?." 1994.

[72] J. R. Schoenherr, R. Thomson, and A. Pyke, "Integrating ethical sensemaking into cybersecurity: A problem-based learning approach," *International Conference on Social Computing, Behavioral-Cultural Modeling & Prediction and Behavior Representation in Modeling and Simulation*, 2020.

[73] R. Senanayake, P. Porras, and J. Kaehler, "Revolutionizing the visual design of capture the flag (ctf) competitions," in *International Conference on Human-Computer Interaction*. Springer, 2019, pp. 339–352.

[74] S. Shrestha, E. Irby, R. Thapa, and S. Das, "Sok: A systematic literature review of bluetooth security threats and mitigation measures," in *International Symposium on Emerging Information Security and Applications*. Springer, 2021, pp. 108–127.

[75] A. Singsa, T. Sriyakul, J. Sutduean, and K. Jermsittiparsert, "Willingness of supply chain employees to support disability management at workplace: A case of indonesian supply chain companies," *Journal of Computational and Theoretical Nanoscience*, vol. 16, no. 7, pp. 2982–2989, 2019.

[76] E. Stowell, M. C. Lyson, H. Saksono, R. C. Wurth, H. Jimison, M. Pavel, and A. G. Parker, "Designing and evaluating mhealth interventions for vulnerable populations: A systematic review," in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems*, 2018, pp. 1–17.

[77] V. Švábenskỳ, J. Vykopal, M. Cermak, and M. Laštovička, "Enhancing cybersecurity skills by creating serious games," in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, 2018.

[78] C. Taylor, P. Arias, J. Klopchic, C. Matarazzo, and E. Dube, "{CTF}:

State-of-the-art and building the next generation," in *2017 {USENIX} Workshop on Advances in Security Education ({ASE} 17)*, 2017.

[79] F. Tazi, J. Dykstra, P. Rajivan, and S. Das, "Sok: Evaluating privacy and security vulnerabilities of patients' data in healthcare," in *proceedings of the 11th International Workshop on Socio-Technical Aspects in Security and Trust STAST*, 2021.

[80] C. Tijus, T.-h. Meen, and C.-y. Chang, *Education And Awareness Of Sustainability-Proceedings Of The 3rd Eurasian Conference On Educational Innovation 2020 (Ecei 2020)*. World Scientific, 2020, vol. 3.

[81] C. Y. Vélez Rodríguez, "Implementation of real-time cybersecurity training through the integration of a hypervisor and an online ctf engine," *Computer Science*, 2018.

[82] V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research*, vol. 11, no. 4, pp. 342–365, 2000.

[83] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management science*, vol. 46, no. 2, pp. 186–204, 2000.

[84] M. P. Vieth, "Cyber operations range [core]: a lightweight and scalable platform for cybersecurity education through gamification," Master's thesis, School of Computing, DePaul University, 2020.

[85] C. Wee, M. Bashir, and N. Memon, "The cybersecurity competition experience: Perceptions from cybersecurity workers," in *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, 2016.

[86] A. Wilkinson, T. Tong, A. Zare, M. Kanik, and M. Chignell, "Monitoring health status in long term care through the use of ambient technologies and serious games," *IEEE journal of biomedical and health informatics*, vol. 22, no. 6, pp. 1807–1813, 2018.

[87] H. Yaxley, "Using new technology effectively in public relations," in *The public relations handbook*. Routledge, 2016, pp. 443–469.

[88] M. J. A. Zahid, M. M. Ashraf, B. T. Malik, and M. R. Hoque, "Information communication technology (ict) for disabled persons in bangladesh: Preliminary study of impact/outcome," in *International Working Conference on Transfer and Diffusion of IT*. Springer, 2013, pp. 652–657.

[89] P. Zaphiris and A. Ioannou, *Learning and Collaboration Technologies. Design, Development and Technological Innovation: 5th International Conference, LCT 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part I*. Springer, 2018, vol. 10924.

[90] L. Zhang-Kennedy and S. Chiasson, "A systematic review of multimedia tools for cybersecurity awareness and education," *ACM Computing Surveys (CSUR)*, vol. 54, no. 1, pp. 1–39, 2021.