Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 1 Article 9

July 2023

A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education

Sherri Weitl-Harms
University of Nebraska at Kearney, harmssk@unk.edu

Adam Spanier
University of Nebraska at Omaha, aspanier@unomaha.edu

John Hastings
University of Nebraska at Kearney, hastingsjd@unk.edu

Matthew Rokusek
University of Nebraska - Lincoln, mrokusek4@huskers.unl.edu

A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education

Abstract

Gamification in education presents a number of benefits that can theoretically facilitate higher engagement and motivation among students when learning complex, technical concepts. As an innovative, high-potential educational tool, many educators and researchers are attempting to implement more effective gamification into undergraduate coursework. Cyber Security Operations (CSO) education is no exception. CSO education traditionally requires comprehension of complex concepts requiring a high level of technical and abstract thinking. By properly applying gamification to complex CSO concepts, engagement in students should see an increase. While an increase is expected, no comprehensive study of CSO gamification applications (GA) has yet been undertaken to fully synthesize the use and outcomes of existing implementations. To better understand and explore gamification in CSO education, a deeper analysis of current gamification applications is needed.

This research outlines and conducts a methodical, comprehensive literature review using the Systematic Mapping Study process to identify implemented and evaluated GAs in undergraduate CSO education. This research serves as both a comprehensive repository and synthesis of existing GAs in cybersecurity, and as a starting point for further CSO GA research. With such a review, future studies can be undertaken to better understand CSO GAs.

A total of 74 papers were discovered which evaluated GAs undergraduate CSO education, through literature published between 2007 and June 2022. Some publications discussed multiple GAs, resulting in a total of 80 undergraduate CSO GAs listing at https://bit.ly/3S260GS. The study outlines each GA identified and provides a short overview of each GA. It also provides a summary of engagement-level characteristics currently exhibited in existing CSO education GAs and discusses common themes and findings discovered in the course of the study.

Keywords

Cybersecurity Education, Gamification, Game-based learning, Pedagogy, Systematic Mapping Study

Cover Page Footnote

An abstract of this article was published in the proceedings of the Conference on Cybersecurity Education, Research & Practice, 2022.

A Systematic Mapping Study on Gamification Applications for Undergraduate Cybersecurity Education

Sherri Weitl-Harms
Cyber Systems Department
University of Nebraska at Kearney
Kearney, NE USA
harmssk@unk.edu
ORCID 0000-0002-3653-2928

Adam Spanier
Information Systems and Technology
University of Nebraska at Omaha
Omaha, USA
aspanier@unomaha.edu
0000-0003-3523-1119

John Hastings
Cyber Systems Department
University of Nebraska at Kearney
Kearney, NE USA
hastingsjd@unk.edu
0000-0003-0871-3622

Matthew Rokusek
School of Computing
University of Nebraska - Lincoln
Lincoln, NE USA
mrokusek4@huskers.unl.edu
0000-0002-0487-2995

***Abstract*—Gamification in education presents a number of benefits that can theoretically facilitate higher engagement and motivation among students when learning complex, technical concepts. As an innovative, high-potential educational tool, many educators and researchers are attempting to implement more effective gamification into undergraduate coursework. Cybersecurity Operations (CSO) education is no exception. CSO education traditionally requires comprehension of complex concepts requiring a high level of technical and abstract thinking. By properly applying gamification to complex CSO concepts, engagement in students should see an increase. While an increase is expected, no comprehensive study of CSO gamification applications (GA) has yet been undertaken to fully synthesize the use and outcomes of existing implementations. To better understand and explore gamification in CSO education, a deeper analysis of current gamification applications is needed.**

This research outlines and conducts a methodical, comprehensive literature review using the Systematic Mapping Study process to identify implemented and evaluated GAs in undergraduate CSO education. This research serves as both a comprehensive repository and synthesis of existing GAs in cybersecurity, and as a starting point for further CSO GA research. With such a review, future studies can be undertaken to better understand CSO GAs.

A total of 74 papers were discovered which evaluated GAs undergraduate CSO education, through literature published between 2007 and June 2022. Some publications discussed multiple GAs, resulting in a total of 80 undergraduate CSO GAs listing at https://bit.ly/3S260GS. The study outlines each GA identified and provides a short overview of each GA. It also provides a summary of engagement-level characteristics currently exhibited in existing CSO education GAs and discusses common themes and findings discovered in the course of the study.

***Index Terms*—Cybersecurity Education, Gamification, Game-based learning, Pedagogy, Systematic Mapping Study**

I. Introduction

Education plays a prominent part in training the innovators responsible for the next generation of technological achievements. In this decade, computer science (CS) occupations alone are forecast to grow 22% [1]. While progress in technology requires well educated students to facilitate its continued growth, technical education often lags behind the pace of technological advancement [2]. This creates an inherently asymmetric relationship between cutting edge technologies and the professionals that will help refine and explore them. Yet, technology cannot wait for education; it must continue to improve.

To short circuit this reactionary feedback loop, education itself must attempt to find innovative technologies, methods, and approaches to more efficiently instruct students [3] and keep pace with new technological advancements. To do this, educators first need to accurately understand the problem. While the increasing pace of technological advancement and the incredible demand placed on education to build better students may frame the issue, the real problem lies in the simple fact that complex ideas are both hard to teach and hard to learn [4]. Though traditional educational approaches can effectively teach complex ideas, the overwhelming volume of new, complex information overburdens traditional approaches in modern education. Simply stated, as technologies become larger, more complex, and more prominent, teaching those technologies becomes exponentially harder.

While the case can be made that traditional text and slide teaching methodologies are easier and faster to develop and implement, the existing asymmetrical relationship between new technologies and effectively educating students to under-

stand them indicates that traditional educational solutions do not effectively solve the problem [2]. Rather than reach for the easiest and fastest means by which to present new information to students, efforts must be undertaken to create frameworks and systems by which educators can more effectively and completely meet the needs of modern education. This approach can be likened to updating a server with new software or replacing old, worn out power plants. Updating old infrastructures can serve in the immediate sense to alleviate operational problems, but the long term ramifications of avoiding new approaches can cause an entire system to deteriorate. While initial investments in time and effort in the development of new educational tools may dwarf traditional presentation slide and text methodologies, the long term outcomes could see educators armed with tools that better fill modern educational needs completely.

One solution to the education problem lies in the use of advanced technological innovations to facilitate more forward-thinking and technological approaches to teaching students. Complex ideas will always be hard to teach, but the means by which these ideas are expressed can be changed to better engage students; new systems can be developed to better meet the requirements that older methods no longer fulfill. New technologies like virtual reality, augmented reality, three-dimensional graphics, interactive content, and advanced modeling can be implemented in educational curriculum in such a way so as to maximize student interactions while minimizing barriers of comprehension [5]. This "gamifying" of education using modern digital technologies shows a great deal of promise in making up lost ground in educational lag.

Gamification is defined by [6] as the use of game elements in inherently non-game environments. This can take a wide variety of forms, but each exhibits game-like characteristics such as leader-boards, badges, competitive elements, cooperation, communication, and advanced computer imaging [7]. Gamification refers to the use of game elements and game design techniques to augment or improve learning [8]. Most significantly, gamification as a practice demonstrates a notable increase in student engagement and motivation when implemented correctly [9]. Due to this increase in student engagement, gamification finds itself at the intersection of a large number of fast growing, technological fields.

One of the fastest growing technological fields in the world today lies in cybersecurity, cybersecurity operations (CSO), and other digital security related disciplines. According to the US Bureau of Labor Statistics, cybersecurity related occupations are slated to increase as much as 33% between 2020 and 2030 [1]. As networks get bigger and faster, as social media sites become more comprehensive, and as our world becomes more digitally connected, cybersecurity and cybercrime will continue to grow at incredible rates [10]. Cybercriminals from all across the globe now pose a threat to all individuals with an internet connection. This new and ever present danger necessitates consistent and intentional efforts among scholars to understand, plan for, and deal with complex cybersecurity issues. Just like other technological fields, the exponential rise of cybersecurity creates an ever increasing lag in education.

Svabensky et al. [11] reviewed CSO education research from 2010-2019 and found that of the 64 papers that describe a teaching intervention, the most common teaching method mentioned in 51 papers is some form of hands-on learning during class time or self-study, including labs, exercises, practical assignments, educational games, and other activities for practicing the selected topic. When considering the integration of new technologies into CSO education, gamification appears to offer benefits to comprehension, engagement, and motivation (Menelaos, 2021). All cyber-attacks occur online or in a digital environment. By using elements of gamification to mock-up, motivate, or emulate these environments, educators can better engage cybersecurity students to understand the complex ideas behind the systems they are attempting to understand.

In an effort to better improve and streamline CSO education to meet industry demand through the use of gamification, a review of existing gamification applications (GAs) used in CSO undergraduate education can provide essential insights into the health and state of gamification in cybersecurity as a whole. As such, this paper presents two main outcomes: 1) an emergent character based classification system for GAs in CSO undergraduate education, and 2) a comprehensive study and categorization of existing GAs utilized and evaluated in CSO undergraduate education.

The rest of the paper is organized as follows. Section 2 delves into the technical background of gamification. Section 3 establishes the research questions and study design used in this study. Section 4 presents the GAs discovered in the literature review. Section 5 provides the discussion. Section 6 details potential future work. Lastly, Section 7 provides conclusions from this research.

II. Background

The use of games in education is as old as education itself. As early as the 7th century BC, the philosopher Plato indicated play "to be necessary for education, as he saw it as a first step on a ladder towards true knowledge" [12]. Lending credibility to the claims made by Plato, renaissance educators such as Goeing (2014) proposed the use of games in subjects like mathematics and science.

While the use of games in education has existed for millennia, the application of digital technologies to modern educational curricula in distinctly "gamified" domains remains significantly less developed. The first recorded proposition of the use of digital technologies in conjunction with educational coursework occurred when a French sociologist named Roger Caillois published a paper called Man, Play, Games [13]. In this paper, Caillois documents observations on social structures and their intrinsic connectivity to games and playfulness. These gamified generalizations were more succinctly connected and explained when "Mark Lepper (1975) and Thomas Malone (1981) first separately presented their analysis of why computer games are engaging and stimulate intrinsic motivation" [12].

The first application of digital technologies to education in a distinctly gamified manner occurred during the CD-ROM era in the 1980's [14]. These early CD-ROMs demonstrated for the first time just how digital technologies could be used in a game-like fashion to help educators reach learning objectives. Though these initial CD-ROM-based applications exhibit very limited educational outcomes, the ideas that drove their design coalesced into a rough grouping of specifically digital and educational gamified applications.

This loose grouping of digital educational games remained only loosely connected until well into 2010 [15]. After late 2010, gamification began gaining traction as a viable area for scholarly research. Gamification as a practice is not quite that of creating a game. Rather, gamification embodies the positive aspects of video games in inherently non-game applications. These positive aspects of the game are considered fun and have the effect of increasing both engagement and motivation in students using them [15]. In an attempt to capture the "fun" brought about by playing video games, educators quickly imagined the benefits that video game elements could generate when paired with educational coursework.

Video game technologies present the unique ability to provide multi-sensory interactions and mission-like experiences to users who play them [16]. In this way, the application of video game technologies to educational curricula can help create multi-sensory environments, resilience building quests, and aspirational simulations into which students can be embedded. This multi-faceted, multi-sensory gamification approach can not only increase motivation and engagement in students [17], but can also generate more motivation for students to stay in notoriously difficult subject areas like mathematics, computer science, and cybersecurity.

CSO are difficult [18] and any tool that can reduce or alleviate the naturally inherent difficulties presented by CSO should be implemented. Gamification, with its mission driven and multi-sensory scope, can help educators better convey the often complex and abstract ideas and environments presented in CSO coursework [19]–[21]. Further, by creating highly engaging user experiences, students can better be retained in and recruited to existing programs [22].

As it stands CSO is woefully under populated. According to [23], the CSO skills crisis is now entering its fifth year, and the outlook isn't improving. "At one point in 2021, there were 500,000 unfilled cybersecurity jobs in the US" (Forbes, 2021). To make the situation worse, Information Security Analyst positions are now the #1 in-demand job in the US with an expected growth of 33% over the next 8 years [1]. Each factor drives home the need to produce more CSO professionals. Due to its attractive nature, engaging and motivating effects, and its ability to convey difficult material, gamification in CSO presents a piece of the puzzle to solve the CSO shortage.

III. Study Design

The literature survey conducted in this research follows a Systematic Mapping Study (SMS) process that has been used by previous studies that mapped gamification applications in related areas [8], [24], [25]. SMS is a secondary study method that systematically (i.e., based on a structured and repeatable process or protocol) explores and categorizes primary studies in a given research field, and provides a structure of the type of research reports and results that have been published [26]. Four researchers participated in the planning and execution of the study: an undergraduate CS student and a graduate student in CSO, and two PhD CS/CSO professors/researchers. The SMS was conducted January-July 2022. The literature survey follows the following process:

- **Step 1 – Research Questions:** The research questions in this study fall into the following broad classifications: 1) Examples, 2) Characteristics, and 3) Conclusions.
- **Step 2 – Literature Review Methodology:** Based on the research questions developed, a transparent, replicable process was implemented to gather generally relevant literature.
- **Step 3 – Literature Selection:** The literature collected was further refined by using a replicable process to select only the most relevant material.
- **Step 4 – Data Extraction:** Based on the research questions and similar to the studies conducted in [25] and [27], the GAs discovered from primary studies were carefully reviewed, and their descriptions were recorded and presented. Common characteristics were noted and discussed.

A. Goals and Research Questions

The goal of this SMS is to identify GAs used and evaluated in undergraduate CSO education for the purpose of understanding their overall general intended value added to the educational experience. To achieve this goal, we establish the following research questions, similar to the research questions outlined in previous studies:

- **RQ1. Examples. What are recent examples of gamification applications used and evaluated in CSO undergraduate education?**
- **RQ2. Characteristics. What characteristics and patterns naturally appear in CSO gamification implementations?**

B. Literature Review Methodology

To answer RQ1, and to facilitate a replicable, robust literature review, a set of search, selection, and analysis processes were designed such that only related literature would find inclusion into this SMS. The methodology follows three primary steps: (1) the literature search, (2) literature selection, and (3) literature analysis. In the literature search, a logical search pattern is used to query targeted databases and create a raw list of potential literature candidates. The literature selection phase sees exclusion and inclusion criteria implemented to generate a relevant corpus of literature. During the analysis phase, pertinent literature will be synthesized, summarized, and categorized according to emergent characteristic patterns among the applications surveyed.

C. Literature Search

The literature search consists of three primary sections: (1) keywords, (2) target databases, and (3) the logical search method. The keywords include terms relevant to gamification, education, and cybersecurity. The target databases are those databases that will be queried for relevant literature. The logical search method is a logical, replicable search string function that utilizes combinations of listed keywords to systematically query targeted databases.

1) Keywords and Terms: The keywords used in this literature review are divided into 3 categories: (1) education, (2) gamification, and (3) undergraduate cybersecurity operations (UCSO). The keywords in each category are as follows:

- Category 1: Education - education, learn, train, course, student, teach
- Category 2: Gamification - game, gamification, game based learning
- Category 3: UCSO - cybersecurity, cyber security, cyber security operations, computer security

2) Database Selection: This study focuses primarily on four databases: (1) IEEE Xplore, (2) The ACM Digital Library, (3) Scopus, and (4) Taylor and Francis. The databases were selected based upon size, popularity, and relevance to the subject and reputation.

A logical, replicable search string function was implemented to systematically query targeted databases. The following logical search string function is used to query the targeted databases. Each query is limited to Abstract only text.

3) Logical Search Method: Search String: Category1 + " AND " + Category2 + " AND " + Category3. In the search string above, one keyword from each keyword category must be chosen and inserted into the search string before committing to the query. A simple combinatorial function will cycle through each unique combination and document the results. We filtered the results of automatic searches to return only papers written in English, and since gamification was not defined until 2011 we excluded papers written before 2005.We filtered based on the paper type of research paper category. Literature not included in this study are: (1) evaluations of labs, (2) physical environment studies, (3) competition studies, (4) tutorials, (5) panels, (6) short studies (two or less pages in length), and (7) posters.

D. Literature Selection

To expand the corpus to particularly relevant related research, citation and reference snowballing was included for the literature that met the filter criteria and related to GAs or Game-based learning in undergraduate CSO education. To stay true to the focus of this study, the data set was refined to only include literature that described an evaluation of the GA or Game-based learning in undergraduate CSO education. Any literature that did not include an evaluation of the GA in CSO education were excluded from the results reported below.

Snowballing is an emerging technique used for conducting systematic literature survey which is efficient and reliable [28]. Snowballing is critical method to find relevant papers, even if the abstract does not contain the required search terms. For this research, the reference lists and citation lists of discovered relevant papers were used to identify new papers to include, following the guidelines established in [29].

E. Data Extraction

Literature that met the criteria were extracted, read and the characteristics of each GA presented and evaluated for undergraduate CSO education were noted and recorded.

IV. Results

A. Overview

A total of 74 papers were discovered which evaluated GAs undergraduate CSO education, through literature published between 2007 and June 2022. Table I shows the source of the GA papers discovered. Some publications, such as [30], discussed multiple GAs, resulting in a total of 80 undergraduate CSO GAs listing at [31].

The studies were published in 47 different venues, with six studies published each in the IEEE Frontiers in Education conference and the USENIX Summit on Gaming, Games, and Gamification in Security Education, followed by three studies published in the ACM Technical Symposium on Computer Science Education. Figure 1 shows the timeline of these studies. Note the continued increase in publications over the past few years, considering that only half of 2022 was included in the study. The individual GAs are described below, in response to RQ1.

TABLE I
Gamification Application Studies in Undergraduate CSO Education

	Base Search	**Unique**	**Met filter criteria**	**Included at least one GA evaluated for UCSO**	**GA evaluated for UCSO**
ACM	89	89	56	8	9
IEEE	121	120	114	12	18
SCOPUS	216	131	125	14	14
Taylor and Francis	7	7	0	0	0
Snowballing	*	*	*	33	33
Totals	433	347	295	67	74

As a means to answer RQ2 and to facilitate the discussion of gamification technologies in undergraduate CSO education, no judgment about the quality and value of the GAs was made, but the explanation provided for the GA and its evaluation in undergraduate CSO education were used. The intended purpose of RQ2 is to understand GAs from a characteristics point of view. That is, using a holistic, qualitative approach rather than a quantitative summation of game elements as referenced by [24] and [32]. Due to the qualitative and emergent nature of RQ2, the answer evolves as CSO gamification applications are discovered and synthesized. The discovered characteristics will be described in the discussion section.

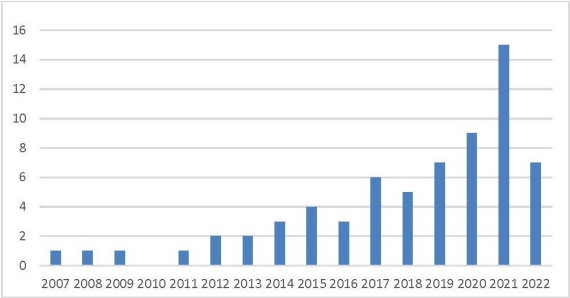

Fig. 1. CSO GA Publications for CSO Undergraduate Education by Year

Similar to the key elements in the game-based learning evaluation model [33], characteristics that are key include: the intended purpose of the GA; the level of engagement the student can experience with the GA; the level of immersion the student can experience within the GA; the level of control the player has to manipulate or co-design the game world; the level of social interaction available in the GA; and the level of self-directedness available in the GA. Common characteristics and patterns discovered in response to RQ2 are provided in the discussion section.

B. CSO Gamification Applications

The generalized education gamification frameworks *Socrative* [34], *Kahoot!* [35], *Seppo* [36], were applied to CSO education [30]. The *OneUP* [37] generalized gamification framework was also applied to CSO education [38].

UltraLearn [39] is a platform similar to *OneUp* that was designed to teach cybersecurity to learners with any background. *GamifiedLearn* [40] is another similar e-learning system.

Shahriar et al. [41] evaluated the *Narrative Integrated Career Exploration (NICE)* platform with a track related to cybersecurity. NICE incorporates certain aspects of gamification including the completion of discreet evolving tasks with attainable rewards.

CYPHER [42] is an open-access MOOC-style learning platform, enabling the delivery of interactive learning content covering essential cryptographic algorithms and their application in security protocols. It has the ability to tailor learning content according to students' needs. Hajja and Hunt [43] present an instruction-based web-platform that allows instructors to create programmable text- and media-based interactive elements and personalized mini-lessons, with gamified elements.

Flushman et al. [44] outline a collection of alternate reality exercises that explore a number of security topics for first year CSO students. The study found improved student engagement with increased awareness of security as a discipline. Similarly, [45] also evaluated various gamified activities for first year CSO students.

Cyber Secured [46] uses engaging gameplay and challenges to educate students about concepts such as phishing, malware, encryption and passwords. It was evaluated in an e-commerce first year course. They found evidence of increased interest in cybersecurity, and positive attitudes towards the use of this game to teach and assess cybersecurity material.

Bodhi [47] is an online two-player game in which each player is shown a piece of code snippet and asked to choose whether their partner would think there is a buffer overflow vulnerability at a given position in the code. At the end of one game, the two players can review all the code snippets for which they do not get the points.

A malware awareness tool, named *MAL-NETS*, was developed and implemented in [48]. From their experience with MALNETS, students who have become aware of malware become cautious of cyber-threats.

Be-aware [49] is a 2D multiple-choice question based quiz game created to cover social engineering concepts, and teach students how to detect and avoid social engineering attacks.

The KMD Puzzle [49] is a 2D image puzzle game that explores content related to key management. The goal of this game is to let students memorize different key management diagrams while they play puzzles and have fun.

A game-based learning platform designed to enhance cybersecurity education is presented in [50]. The platform includes a virtual lab for students to complete the necessary tools for practice and a web portal where all challenges and learning materials are hosted. The aim is to not only help students learn at their own pace about different cybersecurity challenges, but also give them the opportunity to gain hacking skills with ethics taken into mind in a much safer environment.

CounterMeasures [51] is a single player game that provides a game-type environment for learning and practicing security skills through a series of guided missions. As a player completes a mission, the score is incremented according to the difficulty and objectives of the mission. For more difficult missions, the player can seek help, but at the cost of subtracting from the score.

BashDungeon [52] is a game designed with adventure inside a dungeon, aimed at reproducing the topology of a Unix file system. Inside the different rooms, the players can learn how to use several Unix commands, from simple file system actions to complex text manipulations, to complete the quests and win the game.

SherLOCKED [53] is a serious game created in the style of a 2D top-down puzzle adventure. The game is used to consolidate students' knowledge of foundational security concepts (e.g. the CIA triad, security threats and attacks and risk management).

Temple of Treasures [54] is an online 2D educational game that aims to help students learn the basic concepts of Discretionary Access Control and Mandatory Access Control. The game's story is centered around an adventurer who is in search of gold, stuck in a temple, and needing to gain knowledge on targeted concepts to unlock the doors along the escape pathways. It has leader-boards, level controls, and an analytics dashboard.

Bird's Life is a 2D game created to help students understand the concepts of phishing [55].

A "*role-game of the Internet*" game [56] was designed as part of the lab activity of a Network Security course. In this game, instead of fighting against each other, student-teams had to cooperate in order to accomplish a list of business-like tasks over a simulation of the Internet while preserving the security and availability of featured network services.

NITE Team 4 [57] is a commercially available hacking simulation and strategy game with Alternate Reality game elements, was used to enhance learning in Karagiannis & Magkos (2020). The student evaluation was conducted outside the game environment.

Dabrowski et al. [58] introduce students to real-world security attacks and defense mechanisms through a gamified approach used throughout the course. Each challenge is embedded into a small (typically funny) story line including secret missions, big companies, helicopters, or the image of boring office workers turning into computer security superheroes at night.

Zhang et al. [59] created a web-based interactive visualization tool that aims to help students gain a deeper understanding of buffer overflow concepts. It is played as an online game with an analytics dashboard, leader-boards, quizzes, coins and points.

Schreuders and Butterfield [60] created and evaluated an online gamified learning environment, called *My XP*, with all assigned learning activities defined in terms of quests with XP rewards.

Tioh et al. [61] created an adventure game for teaching social engineering concepts. The basic premise of the game places players in the shoes of a penetration tester on his first day on the job, whose typical aim is to infiltrate the building of a fictional business and attempt to steal sensitive corporate and/or technical information.

Image, Preserve, Analyze, and Report (IPAR) (Pan et al., 2017) is a GA that allows students to repeatedly practice forensics tools and reinforce the forensics concepts through detective case studies. Each case is associated with one digital crime scene investigation, and there is a visual representation of the tasks and/or questions to solve each mystery.

Digital Forensics Interactive (DFI) [62] is a 3D game environment to educate users on digital forensics by giving cases to investigate. The user has to follow the normal digital forensics process to solve the case.

Cyberspace Odyssey [63] is a serious game that engages students in a race to successfully perform various cybersecurity tasks in order to collect clues and solve a puzzle in a virtual near-Earth 3D space.

The online game *Werewolves of Miller's Hollow* [64] has been deployed to help students understand information flow. In the game, to avoid being eaten, students must exploit inference channels on a Linux system to discover "werewolves" among a population of "townspeople." Because the werewolves must secretly discuss and vote about who they want to eat at night, they are forced to have some amount of keystroke and network activity in their remote shells at this time. In each instance of the game the werewolves are chosen at random from among the townspeople, creating an interesting dynamic where students must think about information flow from both perspectives and keep adapting their techniques and strategies throughout the semester.

GenCyberCoin [65] is an open-source web platform that provides students with opportunities to earn and spend digital currency, practice bug hunting, and get rewarded for helping peers and completing tasks. This platform introduces students to real-world concepts such as the blockchain, digital currency markets, banks, cybersecurity principles, open source intelligence gathering, passwords, bug bounty, and social norms and values.

Security Requirement Education Game (SREG) [66] is a virtual card game for security requirements education. The game has adaptable maps to give changeability to the game. In one situation, the players are instructed to go and evaluate a particular hospital's organizational and informational settings, obtain vulnerability/weakness and, finally, compromise it by suggesting concrete attack scenarios. The players are working as a team with a common goal to achieve. However, there is competition with other teams. Successful attack scenarios, by analyzing vulnerability and situation for assets, are the winning criteria.

Info-Sec Consultant [49] is a 3D role-playing game similar to CyberProtect designed specifically for CSO undergraduate education. It introduces the logical security techniques to protect computer systems against attacks. The authors also reproduced the traditional board based Snakes and Ladders game in a 2D electronic video game and applied it in the security policy domain.

Ros et al. [67] created a gamification application using storytelling of "*Quantum Corp*". The GA matches the principal cybersecurity concepts with metaphors for the students to solve.

Anti-Phishing Phil [68] (and *Anti-Phishing Phyllis* [69]) were developed at Carnegie Mellon University to provide user-friendly tools to teach about phishing attacks. In the *Anti-Phishing Phil* game, players have to guide a fish towards different worms that will display a genuine or a phishing link. In the *Anti-Phishing Phyllis* game, players help Phyllis teach her school of fish how to avoid phishing traps in fraudulent emails. Unfortunately, *Anti-Phishing Phyllis* was not evaluated for undergraduates, and is not included in the count in Table I.

Cybersecurity virtual escape rooms provide for fun gamified applications [70]–[75]. Borrego et al. [70] created an escape room game activity in an Information and Security course, for students to learn concepts such as information measurement, data compression techniques, cryptography, privacy, authenticity, accessibility and public key and private key infrastructure. Deeb and Hickey [72] created a 3D Escape Room game for introducing computer security and cryptography. *CySecEscape 2.0* [73] is a virtual escape room addressing the cybersecurity challenges of small and medium-size companies, based on an earlier version of the system created as a physical escape room. Williams [75] created a concept map that outlined

the relationships of gamification, escape rooms, and learning skills to help future researchers transition content to virtual escape room environments. Their model incorporated the cybersecurity-related skills of social engineering, password security, and binary to create a collaborative virtual experience. DeBello et al. [71] created *Escape the Classroom* that covered many CSO concepts and Taladriz [74] created an escape room activity to cover networking concepts.

The *EDURange* framework [76] is a cloud-based resource for hosting on-demand interactive cybersecurity scenarios. The scenarios they have implemented were designed specifically to nurture the development of analysis skills in students as a complement to both theoretical security concepts and specific software tools. They implemented several exercises in the framework, including exercises for students to learn about mapping a network and understanding network protocols, such as TCP, UDP, ICMP; and exercises for students to learn about intrusion detection and prevention; exercises for students to learn about forensics and reverse engineering; exercises where the players must find data on a target host that is behind a gateway by passively examining network traffic and crafting packets to reveal specific information in a text-based adventure; exercises where the player has to create a set of rules to control traffic in and out of a network; exercises where the defender is given the grammar for a calculator and must implement an interpreter for that grammar and the attacker tries to fuzz the interpreter to produce incorrect results or get it to reject a valid expression; and exercises where students learn to filter large amounts of data to distinguish between normal and anomalous behavior indicative of malware.

hACME is a GA that aims to teach students software security, specifically within web applications, implemented by Nerbraten and Rostad [77]. Each player works through a series of levels where the goal is to discover the vulnerabilities or flaws in a given HTML page in order to unlock access to the next stage. Upon unlocking a new level, all challenges within the level are immediately available. This allows students to pick their own path to the next level. Users can use hints to work through difficult problems, and, as they progress, are awarded points for completing each challenge. These points are then used to rank the player on a leader-board.

Morreale et al. [78] implement a generalized, gamified pathway for CS students to visualize their progress in any CS major program including CSO. A game-board depicts necessary tasks required for each academic year. Badges are also awarded for different pathways. These include the Ready to Succeed badge, the Road to Graduate School badge, and Academic Mage badges.

Riposte [79] is a framework for measuring skills demonstrated by students within an active learning setting where the primary focus is on practical expertise. The gamified framework is insecure enough to be "hackable", but secure enough not to be abused and is used to expose students to various security concepts.

In research carried out by [80], a fictional story is used, where students play the part of a new IT security employee at a company and are asked to complete a number of security tasks. In response to completing these tasks, each student receives a flag. The students can send the flags they find to a number of different characters to move the story along in different ways. As the story unfolds they find deceit, corruption and ultimately murder, and their choices lead them to one of three different endings.

Playground [81] is a network security simulation and training tool. Students use Playground to create their own network security architecture, almost from the ground up. Upon the completion of a given topology, the students then turn around and figure out all the different ways they might crack it.

PenQuest [82] is a meta model designed to present a complete view on information system attacks and their mitigation while simultaneously providing a tool for both semantic data enrichment and security education. It simulates time-enabled attacker/defender behavior as part of a dynamic, imperfect information multiplayer game that derives significant parts of its ruleset from established information security sources. Attack patterns, vulnerabilities, and mitigating controls are mapped to counterpart strategies and concrete actions. The gamified model considers and defines a wide range of actors, assets, and actions, thereby enabling the assessment of cyber-risks while giving technical experts the opportunity to explore specific attack scenarios in the context of an abstracted IT infrastructure.

Cybermatics is an interactive simulation that allows students to "play" through an authentic scenario (case study) as a member of a professional team [83]. The applications saw increased student understanding about certain key aspects of professional cybersecurity work, improved their confidence in being able to successfully apply certain skills associated with cybersecurity, and increased nearly half of the students' interest in pursuing a cybersecurity career [83].

Simulated Critical Infrastructure Protection Scenarios (SCIPS) [84] is an experiential serious game utilized to shape the risk thinking of participants with respect to different cybersecurity scenarios in order to train situational awareness and mental models for incident response. The SCIPS platform is data-driven for cross-extensibility allowing it to be adapted to a whole range of different training requirements.

Koch et al. [85] present a cybersecurity educational application that features a game goal unrelated to IT security. However, during the game session gradually more and more attacks on the underlying infrastructure disturb game play. Such a scenario is very close to the reality of an IT security expert, where establishing security is just a necessary requirement to reach the company's goals.

Alothman et al. [86] present a *Kuwait cyber-range (Q8CR)* that runs a cybersecurity attack and defense simulation, with red and blue teams that work against each other, and a black team that is responsible for creating and evaluating the scenario cases for both the red and blue teams. This, and other cyber range activities, such as [87] contain many gamification characteristics.

CyberCIEGE [88] is a popular security awareness tool that

was developed by the Naval Postgraduate School and other collaborators and has been used extensively in cybersecurity education [60], [89]. The game offers realistic virtual world scenarios in which players have to operate and defend a computer network.

QuaSim [90] is designed to educate junior/senior undergraduate and graduate students in quantum cryptographic principles. It poses quantum cryptographic problems developed by domain experts and students are able to interactively find solutions to them. QuaSim facilitates collaborative and competitive project-based student learning of quantum principles.

Space Fighter [49] is a 3D action/adventure game designed to cover phishing attack techniques as well as different types of malware. These authors also created *Hacking Simulator* [49], a 2D simulation game designed to simulate network attacks and teach students basic IP/TCP attacks against computer networks.

A Capture the Flag (CTF) competition is a special kind of information security competition. There are three common types of CTFs: Jeopardy, Attack-Defense and mixed [91]. Jeopardy-style CTFs have questions (tasks) in a range of categories, such as web, forensic, crypto, etc. Teams gain points for every solved task, and typically more points for more complicated tasks. At the end of the game time, the sum of points shows the CTF winner. One famous example of such CTF competitions are the Defcon CTF qualifiers [92]. In an attack-defense CTF, either one or both teams has its own network with vulnerable services. Each team has a limited time to patch their services and develop exploits before CTF competition organizers connect the participants and the wargame starts. Teams try to protect their own services for defense points and hack opponents for attack points. Historically this is the first type of CTF. The most famous example lies in the DEF CON CTF [93] competition. Mixed CTF competitions have various possible formats. They may be something like a wargame with special time for task-based elements, e.g. the International Capture The Flag (iCTF) competition [94]. Backman [95] and Carlisle et al. [96] present details on how to deploy and organize a CTF competition for undergraduate students.

Karagiannis & Magkos (2021) [97] used a CTF framework and challenges through a linear sequence while simultaneously presenting educational context for the students to engage gradually and acquire the appropriate knowledge and skills.

Two Jeopardy-style CTFs were used and evaluated in CSO education in [98]. The CTF competitions consisted of challenges covering several security topics, but did not have a specific scenario or context for the applications. Similarly, a virtual-machine (VM) based CTF framework was created by Chothia & Novakovic [80], for CSO students to complete Jeopardy-style CTF challenges. They also focused on technical skills and understanding and were not based on a specific scenario. For all exercises, students were required to submit written answers describing the steps they took to recover flags from the VM, and — where appropriate — a description of what the vulnerabilities were and how they worked, and an explanation of how they could be fixed.

Incorporating the *CyberChallenge.IT*, a jeopardy-style CTF that is the leading Italian initiative for introducing young talents to the field of cybersecurity, into undergraduate curriculum [99] was discussed and evaluated in [100].

Vitorino et al. [101] presented *StarsCTF*, a Capture the Flag experiment designed to assess player types and their levels of engagement. In a paired experiment, an individual Jeopardy format (called Open World) was used, and a new game mode was developed, called DMC (Dynamics, Mechanics and Components). "The Open World's challenges have elements to satisfy players with high scores in the player type achievement (Challenges, Feedback and Points), and DMC ones have elements to satisfy achievement and immersion player types (Narrative, Progression Restrictions, Challenges, Feedback and Points)." [101]

Kornegay et al. [102] evaluated the *MITRE eCTF*, which takes "a systems approach to security, i.e., it considers both the hardware and the software counterparts under consideration for security analysis." The *eCTF* framework also " provides a balanced approach to cyber-attack and defense strategies." They found that the *eCTF* "allowed students to work in teams, develop critical thinking skills, address complex technical issues associated with real-world applications, and motivate continued learning, and increased research productivity after the course ended."

Facebook's CTF platform has also been used as a learning and assessment tool in CSO education [30], [103].

GeoCTF [104] is an educational CTF-style tool designed to raise the level of awareness about the dangers of uncontrolled sharing of location data, and to illustrate prominent location protection techniques.

SWaT Security Showdown (S3) [105] was a gamified CTF event that was specifically targeted at Industrial Control Systems (ICS) security. S3 implemented challenges that include both theoretical and applied ICS security concepts, using simulated and real ICS infrastructures. The competition included international teams of attackers and defenders both from academia and industry.

A cloud-based election application provides the scenario for a CTF activity designed to teach students about the potential pitfalls and consequences of cloud misconfiguration [106]. Students pose as malicious actors who seek to compromise an election application running on a cloud environment.

Another CTF example [107] focuses on a radical animal rights group's wishes to free an animal held in zoo captivity. Their goal in this attack is to compromise access to the zoo's website and then delete animals from the zoo's inventory database. The challenge is divided into three phases that mimic an actual penetration testers methodology: a reconnaissance phase, an exploitation phase, and an execution phase.

Broholm et al. [108] evaluated three cybersecurity training platforms Haaukins [109], HackTheBox [110], and picoCTF [111]. Haaukins is an "immersive, interactive learning platform, which allows students hands-on, practical experience with cybersecurity and ethical hacking in an online, virtual-

ized environment." Hack the Box is a cybersecurity training platform based on a capture the flag style competition that is always available. PicoCTF is a two week competition that everyone can enter to compete.

PeerSpace is a network based collaborative learning environment created by Li et al. [112]. *PeerSpace* utilizes elements like peer review, project repositories, wikis, profiles, friends, blogs and discussions to build relationships and encourage collaboration between students. It also provides a game section which students can use to better understand the coursework.

Classroom Live is an undergraduate level GA created for CS students, including CSO students. In the development of this software, students and teachers work together to create an application for communicating generalized CS coursework [113].

Code Defenders [114] is used to teach software testing in a collaborative way. Attackers create mutant versions of the program and defenders write test cases for the program being tested. As players progress through levels of the game, they incrementally learn and practice testing concepts.

In a study by Svabensky et al. [115], students participate in a game-development based learning project that sees the individual creation of different penetration testing games. The students report they enjoyed a unique opportunity to deeply understand the topic and practice their soft skills as they presented their results at a faculty open day event. Their peers, who played the created games, rated the quality and educational value of the games as overwhelmingly positive. While the application of this process sees students interacting with unrelated static gamification iterations, the game development pre-phase contains GA elements.

McGregor et al. [116] presented the *Citadel Programming Lab* which comprises a GitLab instance for simulated secure programming tasks and a tower defense game. In this game environment, students first play the tutorial level, which exposes them to the purpose of game and gameplay mechanics. This is followed by the students playing the main level, which exposes them to security metaphors, helps them develop motivation to defend their goal and allows them to earn points. Students can then spend points to unlock upgrades, which some upgrade tiers require solving a programming task and reviewing other solutions.

In a study by Celeda et al. [117], students participate in a game-development based learning project where paired students create CTF games that are deployed to the Kypoindustry industrial control systems testbed. Then a public hacking day is organized for other students of the university to play the created games. Unfortunately, because the study does not provide an evaluation of the impact of this activity on the students, it is not included in the reported results in Table I.

V. Discussion

By carrying out the literature review outlined above to create a CSO GA based research corpus, recent examples of CSO Gamification were collected and evaluated. The resulting research corpus and identified CSO GAs served to answer RQ1.

In terms of the literature search process, there were several papers discovered that met the search criteria but did not include an evaluation of a GA in undergraduate education. This required the researchers to read and evaluate a large number of papers that met the search criteria (433) to discover 41 (55%) of the relevant 74 studies on undergraduate CSO GAs reported.

For the 295 papers found to meet the criteria as shown in Table I, their citations and references were reviewed via snowballing. Often these papers were close enough to require their citations and references to also be reviewed, in a second-level of the snowballing method. Snowballing continued in this fashion until no new related literature was found. The multi-phase snowballing method resulting in hundreds of additional papers reviewed, which are not included in the first three columns of Table I. In total, nearly a thousand papers related to gamification in cybersecurity education were reviewed.

The snowballing method lead to the discovery of 38 (51%) of the 74 relevant GA studies discovered. There were a handful of ACM/IEEE papers that were found by snowballing, as their abstract did not contain the search terms. For example, Deeb & Hickey (2019)'s IEEE paper on a 3D escape room was found via snowballing. Because the escape room has GA elements and was used in CSO undergraduate education, this paper was included in this study. Another potential cause for the large number of the relevant GAs to be discovered via snowballing, is that CSO education publication venues are varied (47 in total). Additionally, several of the venues were not included in the databases used, including the USENIX Summit on Gaming, Games, and Gamification in Security Education, where six studies were published, the *Journal of Cybersecurity Education, Research and Practice* and the *International Journal of Serious Games*. Thus, for this research, the snowballing technique was used to discover a relatively large percentage of the overall literature reported.

After reviewing the CSO GAs collected in this study, common characteristic patterns emerged, in response to RQ2.

Tests and quizzes by their very nature tend to be tedious and disengaging. Several GAs attempt to engage students within the context of an exam, quiz, or homework by providing a graphically attractive and/or interactive interface [27]. Typically, the level of engagement, immersion and control that the student has in these kinds of GAs is low.

Several CSO education GAs add a story line and well-defined step-by-step processes that enable students to complete quests as they progressively learn content. These GAs derive their main characteristics from the required steps needed to take to reach the conclusion. The level of engagement, immersion and control that the student can experience with these GAs is typically higher than GAs designed for testing purposes, even though these types of GAs also typically include a means to evaluate student learning.

Many CSO education GAs utilize visualization to describe abstract ideas [27]. Visualizations can assist students with

understanding abstract ideas that are difficult to comprehend. Additionally, these visualizations can allow instructors to demonstrate a step-by-step walk-through of the abstract idea, effectively and flexibly. The level of engagement, immersion, and control that the student can experience with GAs with these characteristics is typically similar to the mission-based GAs.

Simulations provide environmental ambiance and context, oftentimes via immersive content, into which narrative and story are integrated to bolster engagement [118]. In simulations, players are free to move around and explore the environment. The level of engagement, immersion and control that the student can experience with these kinds of GAs is typically higher than mission-based GAs. Several CSO education GAs are simulations.

In CSO education, many educators make use of goal driven simulations, test-beds and competitions to augment student learning [88], [90], [91], [94]. With these kinds of GAs, no predefined step-based process is required; the student simply needs to accomplish some goal in any way possible as fast as possible. Some, but not all, of these applications employ game mechanics such as: points, levels, paths and progress, challenges, immediate feedback, leader-boards, gifts and sharing, badges, and time restrictions. The level of engagement, immersion and control that the student can experience with these GAs is typically higher than mission-based GAs as the tasks are typically more challenging.

Some GAs have social and collaborative engagement characteristics to allow students to regularly and easily interact such that student motivation and engagement is improved [27]. The level of engagement, immersion and control that the student can experience with these GAs is typically similar to the mission-based GAs, but the social and collaborative engagement is much higher.

A few CSO GAs dynamically change according to user input throughout its gamified life cycle, enabling students to take ownership of the gamification experience.

VI. Future Work

Based on the findings discovered in this CSO study, the researchers intend to focus on a number of notable areas of interest pertaining to characteristic-based gamification. More specifically, the researchers intend to focus on more concise, accurate, and comprehensive characteristic-based frames to organize the GAs into groupings. Specifically, we will look at what constructs exist that are useful in identifying and organizing the intrinsic characteristics of gamification systems for CSO education. The characteristics and patterns that naturally provide order and structure for CSO gamification implementations need to be identified. Then, each CSO gamification implementation needs to be grouped according to common characteristics. The answers to these questions are forthcoming from the researchers.

A comprehensive study of gamification applications in computer science undergraduate education is also forthcoming from the researchers. This includes using additional databases, such as ProQuest. The authors would like to develop an online repository of digital CS education GAs/Frameworks, with incentives for experts/developers to add their GAs to the repository, searchable metadata, and links to source/implementations.

VII. Conclusion

A literature review of gamification applications in undergraduate CSO education is useful in determining the current state of a very fast-growing discipline. To best direct this currently uninhibited growth, regular effort should be made by researchers to design and develop GAs that better fit into the disciple as a whole.

While gamification is prevalent in all facets of CS education, its application in the fast-growing field of CSO provides valuable insights as to the focus and intent of gamification researchers in CSO related fields. A broad understanding of where effort is being placed in CSO gamification development can help researchers better gauge which areas in CSO gamification need more attention.

Preliminary findings in this research demonstrate that there are a large number of GAs that have been evaluated in undergraduate CSO education. A more comprehensive study is forthcoming, however, these findings generate enough data to indicate that there is a high likelihood that, with minor adjustments, the framework scheme as proposed in [27] will appropriately classify both CSO education GAs as well as GAs that fit into the broader scope of computer science undergraduate education.

References

[1] Bureau of Labor and Statistics, "Information security analyst," 2022, accessed: March 10, 2022. [Online]. Available: https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[2] C. Goldin and L. F. Katz, *The race between education and technology*. Cambridge, MA: Harvard University Press, 2010.

[3] A. Kirkwood and L. Price, "Examining some assumptions and limitations of research on the effects of emerging technologies for teaching and learning in higher education," *British Journal of Educational Technology*, vol. 44, no. 4, pp. 536–543, 2013.

[4] A. Wentzel, *Teaching Complex Ideas: How to Translate Your Expertise into Great Instruction*. Milton Park, Oxfordshire, England, UK: Routledge, 03 2019. ISBN 9781351058117

[5] L. Annetta, J. Mangrum, S. Holmes, K. Collazo, and M.-T. Cheng, "Bridging realty to virtual reality: Investigating gender effect and student engagement on learning through video game play in an elementary school classroom," *International Journal of Science Education*, vol. 31, no. 8, pp. 1091–1113, 2009.

[6] 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.

[7] S. Villagrasa, D. Fonseca, E. Redondo, and J. Duran, "Teaching case of gamification and visual technologies for education," *Journal of Cases on Information Technology (JCIT)*, vol. 16, no. 4, pp. 38–57, 2014.

[8] M. R. d. A. Souza, L. F. Veado, R. R. Moreira, E. M. L. Figueiredo, and H. Costa, "A systematic mapping study on game-related methods for software engineering education," *Information and Software Technology*, vol. 95, pp. 201–218, 2018.

[9] S. Sandusky, "Gamification in education," 2015.

[10] T. Riley, "The cybersecurity 202: Cybercrime skyrocketed as workplaces went virtual in 2020, new report finds," 2021, accessed: March 10, 2022. [Online]. Available: https://www.washingtonpost.com/politics/2021/02/22/cybersecurity-202-cybercrime-skyrocketed-workplaces-went-virtual-2020/

[11] V. Švábenský, J. Vykopal, and P. Čeleda, "What are cybersecurity education papers about? a systematic literature review of SIGCSE and ITiCSE conferences," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '20. New York, NY, USA: Association for Computing Machinery, 2020. doi: 10.1145/3328778.3366816. ISBN 9781450367936 p. 2–8.

[12] A. Hellerstedt and P. Mozelius, "Game-based learning: A long history," in *Irish Conference on Game-based Learning 2019, Cork, Ireland, June 26-28, 2019*, vol. 1. Cork, Ireland: Irish Conference on Game-Based Learning, 2019, pp. 1–4.

[13] A. Pandey, "A brief history of gamification," *XRDS*, vol. 24, no. 1. doi: 10.1145/3123774 p. 13, Sep. 2017.

[14] K. Becker and S. Nicholson, "Gamification in the classroom: Old wine in new badges," *Learning, education and games*, vol. 61, pp. 61–85, 2016.

[15] B. Kim, "Gamification," *ALA TechSource*, vol. 51. doi: 10.5860/ltr.51n2 pp. 10–18, 2 2015.

[16] C.-H. S. Chang, C.-C. Kuo, H.-T. Hou, and J. J. Y. Koe, "Design and evaluation of a multi-sensory scaffolding gamification science course with mobile technology for learners with total blindness," *Computers in Human Behavior*, vol. 128, p. 107085, 2022.

[17] R. S. Alsawaier, "The effect of gamification on motivation and engagement," *The International Journal of Information and Learning Technology*, vol. 35, no. 1, pp. 56–79, 2018.

[18] A. Minnaar, "'crackers', cyberattacks and cybersecurity vulnerabilities: the difficulties in combatting the'new'cybercriminals," *Acta Criminologica: African Journal of Criminology & Victimology*, vol. 2014, no. sed-2, pp. 127–144, 2014.

[19] M. Y. Alghamdi and Y. A. Younis, "The use of computer games for teaching and learning cybersecurity in higher education institutions," *Journal of Engineering Research (Kuwait)*, vol. 9, no. 3. doi: 10.36909/jer.v9i3A.10943 p. 143 – 152, 2021.

[20] K. Boopathi, S. Sreejith, and A. Bithin, "Learning cyber security through gamification," *Indian Journal of Science and Technology*, vol. 8, no. 7, pp. 642–649, 2015.

[21] C. Li and R. Kulkarni, "Survey of cybersecurity education through gamification," in *ASEE Annual Conference and Exposition, Conference Proceedings*, vol. 2016-June, 2016, Conference paper.

[22] M. Janosz, I. Archambault, J. Morizot, and L. S. Pagani, "School engagement trajectories and their differential predictive relations to dropout," *Journal of social Issues*, vol. 64, no. 1, pp. 21–40, 2008.

[23] Information Systems Security Association, "Cybersecurity skills crisis continues for fifth year, perpetuated by lack of business investment," https://www.issa.org/cybersecurity-skills-crisis-continues-for-fifth-year-perpetuated-by-lack-of-business-investment/, 2021, accessed: March 10, 2022.

[24] D. Dicheva, C. Dichev, G. Agre, and G. Angelova, "Gamification in education: A systematic mapping study," *Educational technology & society*, vol. 18, no. 3, pp. 75–88, 2015.

[25] R. H. B. Monteiro, S. R. B. Oliveira, and M. R. De Almeida Souza, "A standard framework for gamification evaluation in education and training of software engineering: an evaluation from a proof of concept," in *IEEE Frontiers in Education Conference (FIE)*, Lincoln, NE, 2021. doi: 10.1109/FIE49875.2021.9637232 pp. 1–7.

[26] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Information and Software Technology*, vol. 64, pp. 1–18, 2015.

[27] A. M. Spanier, S. K. Weitl-Harms, and J. D. Hastings, "A classification scheme for gamification in computer science education: Discovery of foundational gamification genres in data structures courses," in *IEEE Frontiers in Education Conference (FIE)*, Lincoln, NE, 2021, pp. 1–9.

[28] P. Juneja and P. Kaur, "Software engineering for big data application development: Systematic literature survey using snowballing," in *2019 International Conference on Computing, Power and Communication Technologies (GUCON)*, 2019, pp. 492–496.

[29] C. Wohlin, "Guidelines for snowballing in systematic literature studies and a replication in software engineering," in *Proceedings of the 18th international conference on evaluation and assessment in software engineering*, 2014, pp. 1–10.

[30] M. Beltrán, M. Calvo, and S. González, "Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs," in *2018 International Conference on Computational Science and Computational Intelligence (CSCI)*. Las Vegas, NV: CSCI, 2018. doi: 10.1109/CSCI46756.2018.00116 pp. 574–579.

[31] S. K. Weitl-Harms, A. M. Spanier, and J. D. Hastings, "CSO gamification application listing 2022," https://bit.ly/3S260GS, 2022.

[32] K. Werback and D. Hunter, *The Gamification Toolkit*. Philadelphia, PA: Wharton School Press, 2015.

[33] E. Oprins, G. Visschedijk, M. B. Roozeboom, M. Dankbaar, W. Trooster, and S. C. Schuit, "The game-based learning evaluation model (gem): measuring the effectiveness of serious games using a standardised method," *International Journal of Technology Enhanced Learning*, vol. 7, no. 4, pp. 326–345, 2015.

[34] Showbie Inc., "Sacrative," 2022, accessed: 2022-03-14. [Online]. Available: https://www.socrative.com/

[35] Kahoot!, "Kahoot!" 2022, accessed: 2022-03-14. [Online]. Available: https://kahoot.it/

[36] Seppo, "Seppo," 2021, accessed: 2022-03-14. [Online]. Available: http://seppo.io/

[37] D. Dicheva, K. Irwin, and C. Dichev, "OneUp learning: A course gamification platform," in *GALA*. Switzerland: Springer, 2017, pp. 1–11.

[38] F. Demmese, X. Yuan, and D. Dicheva, "Evaluating the effectiveness of gamification on students' performance in a cybersecurity course," *Journal of the Colloquium for Information System Security Education*, vol. 8, no. 1, pp. 1–12, 2020. [Online]. Available: https://par.nsf.gov/biblio/10290874

[39] S. Raisi, S. Ghasemshirazi, and G. Shirvani, "UltraLearn: Next-generation cybersecurity learning platform," in *2021 12th International Conference on Information and Knowledge Technology (IKT)*, 2021. doi: 10.1109/IKT54664.2021.9685940 pp. 83–88.

[40] M. T. Alshammari, "Design and learning effectiveness evaluation of gamification in e-learning systems," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 9. doi: 10.14569/ijacsa.2019.0100926 p. 204 – 208, 2019.

[41] S. Shahriar, J. Ramesh, M. Towheed, T. Ameen, A. Sagahyroon, and A. R. Al-Ali, "Narrative integrated career exploration platform," *Frontiers in Education*, vol. 7. doi: 10.3389/feduc.2022.798950 2022.

[42] Y. A. Younis, K. Kifayat, Q. Shi, E. Matthews, G. Griffiths, and R. Lambertse, "Teaching cryptography using cypher (interactive cryptographic protocol teaching and learning)," in *Proceedings of the 6th International Conference on Engineering & MIS 2020*, ser. ICEMIS'20. New York, NY, USA: Association for Computing Machinery, 2020. doi: 10.1145/3410352.3410742. ISBN 9781450377362

[43] A. Hajja and A. J. Hunt, "A novel e-learning platform for building and publishing student-driven personalized lessons," in *2020 IEEE Frontiers in Education Conference (FIE)*. Uppsala, Sweden: IEEE, 2020. doi: 10.1109/FIE44824.2020.9274034 pp. 1–8.

[44] T. Flushman, M. Gondree, and Z. N. J. Peterson, "This is not a game: Early observations on using alternate reality games for teaching security concepts to First-Year undergraduates," in *8th Workshop on Cyber Security Experimentation and Test (CSET 15)*. Washington, D.C.: USENIX Association, Aug 2015, pp. 1–8. [Online]. Available: https://www.usenix.org/conference/cset15/workshop-program/presentation/flushman

[45] R. K. Dixit, M. Nirgude, and P. S. Yalagi, "Employ gamification to make "i&cs" more interesting," *Journal of Engineering Education Transformations*, vol. 32, no. 2, p. 55 – 60, 2018.

[46] D. Kletenik, A. Butbul, D. Chan, D. Kwok, and M. LaSpina, "Game on: Teaching cybersecurity to novices through the use of a serious game," *J. Comput. Sci. Coll.*, vol. 36, no. 8, p. 11–21, apr 2021.

[47] J. Chen and X. Mao, "Bodhi: Detecting buffer overflows with a game," in *2012 IEEE Sixth International Conference on Software Security and Reliability Companion*. Gaithersburg, Maryland: IEEE, 2012. doi: 10.1109/SERE-C.2012.35 pp. 168–173.

[48] N. S. Omar, C. Foozy1, I. Hamid, H. Hafit, A. Arbain, and P. Shamala, "Malware awareness tool for internet safety using gamification techniques," *Journal of Physics: Conference Series*, vol. 1874, pp. 1–9, 2021.

[49] M. Mostafa and O. S. Faragallah, "Development of serious games for teaching information security courses," *IEEE Access*, vol. 7. doi: 10.1109/ACCESS.2019.2955639 pp. 169 293–169 305, 2019.

[50] M. Khan, A. Merabet, and S. Alkaabi, "Game-based learning platform to enhance cybersecurity education," 2022.

[51] C. Jordan, M. Knapp, D. Mitchell, M. Claypool, and K. Fisler, "CounterMeasures: A game for teaching computer security," in *2011 10th Annual Workshop on Network and Systems Support for Games*. Ottawa, Canada: ACM, 2011. doi: 10.1109/NetGames.2011.6080983 pp. 1–6.

[52] F. Corda, M. Onnis, and M. e. a. Pes, "BashDungeon," *Multimed Tools Appl*, vol. 78. doi: 10.1007/s11042-019-7230-3 p. 13731–13746, 2019.

[53] A. Jaffray, C. Finn, and J. Nurse, "SherLOCKED: A detective-themed serious game for cyber security education," in *Human Aspects of Information Security and Assurance, HAISA 2021*, vol. 613, 2021. doi: 10.1007/978-3-030-81111-2_4 pp. 34–45.

[54] P. Weanquoi, J. Zhang, X. Yuan, J. Xu, and E. J. Jones, "Learn access control concepts in a game," in *2021 IEEE Frontiers in Education Conference (FIE)*. Lincoln, NE: IEEE, 2021. doi: 10.1109/FIE49875.2021.9637228 pp. 1–6.

[55] P. Weanquoi, J. Johnson, and J. Zhang, "Using a game to improve phishing awareness," *Journal of Cybersecurity Education, Research and Practice*, vol. 2018, no. 2, pp. 1–14, 2018. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2018/iss2/2

[56] L. Catuogno and A. De Santis, "An internet role-game for the laboratory of network security course," in *Proceedings of the 13th Annual Conference on Innovation and Technology in Computer Science Education*, ser. ITiCSE '08. New York, NY, USA: Association for Computing Machinery, 2008. doi: 10.1145/1384271.1384336. ISBN 9781605580784 p. 240–244.

[57] Alice and Smith, "NITE Team 4," https://www.niteteam4.com, 2022, accessed: March 10, 2022.

[58] A. Dabrowski, M. Kammerstetter, E. Thamm, E. Weippl, and W. Kastner, "Leveraging competitive gamification for sustainable fun and profit in security education," in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. Washington, D.C.: USENIX Association, Aug 2015, pp. 1–8. [Online]. Available: https://www.usenix.org/conference/3gse15/summit-program/presentation/dabrowski

[59] J. Zhang, X. Yuan, J. Johnson, J. Xu, and M. Vanamala, "Developing and assessing a web-based interactive visualization tool to teach buffer overflow concepts," in *2020 IEEE Frontiers in Education Conference (FIE)*. Lincoln, NE: IEEE FIE, 2020. doi: 10.1109/FIE44824.2020.9274239 pp. 1–7.

[60] Z. C. Schreuders and E. Butterfield, "Gamification for teaching and learning computer security in higher education," in *2016 USENIX Workshop on Advances in Security Education (ASE 16)*, Austin, TX, Aug 2016, pp. 1–8. [Online]. Available: https://www.usenix.org/conference/ase16/workshop-program/presentation/schreuders

[61] J.-N. Tioh, M. Mina, and D. W. Jacobson, "Cyber security social engineers an extensible teaching tool for social engineering education and awareness," in *2019 IEEE Frontiers in Education Conference (FIE)*. Cincinatti, OH: IEEE, 2019. doi: 10.1109/FIE43999.2019.9028369 pp. 1–5.

[62] J. Yerby, S. Hollifield, M. Kwak, and K. Floyd, "Development of serious games for teaching digital forensics," *Issues in Information Systems*, vol. 15, no. 2, pp. 335–343, 2014.

[63] K. Graham, J. Anderson, C. Rife, B. Heitmeyer, P. R. Patel, S. Nykl, A. C. Lin, and L. D. Merkle, "Cyberspace Odyssey: A competitive team-oriented serious game in computer networking," *IEEE Transactions on Learning Technologies*, vol. 13, no. 3. doi: 10.1109/TLT.2020.3008607 pp. 502–515, 2020.

[64] R. Ensafi, M. Jacobi, and J. R. Crandall, "Students who don't understand information flow should be eaten: An experience paper," in *CSET*. Belleview, WA: CSET, 2012, pp. 1–10.

[65] V. Ford and A. Siraj, "GenCyberCoin: An engaging, customizable, and gamified web platform for cybersecurity summer camps and classrooms," *J. Comput. Sci. Coll.*, vol. 35, no. 3, p. 87–96, oct 2019.

[66] A. Yasin, L. Liu, T. Li, J. Wang, and D. Zowghi, "Design and preliminary evaluation of a cyber Security Requirements Education Game (SREG)," *Information and Software Technology*, vol. 95, pp. 179–200, 2018.

[67] S. Ros, S. González, 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. doi: 10.1109/ACCESS.2020.2996361 pp. 97 718–97 728, 2020.

[68] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge, "Anti-Phishing Phil: The design and evaluation of a game that teaches people not to fall for phish," in *Proceedings of the 3rd Symposium on Usable Privacy and Security*, ser. SOUPS '07. New York, NY, USA: Association for Computing Machinery, 2007. doi: 10.1145/1280680.1280692. ISBN 9781595938015 p. 88–99.

[69] Carnegie Mellon University, "Anti-Phishing Phyllis," 2022, accessed: March 10, 2022. [Online]. Available: https://www.cmu.edu/iso/aware/phyllis/index.html

[70] C. Borrego, C. Fernández, I. Blanes, and S. Robles, "Room escape at class: Escape games activities to facilitate the motivation and learning in computer science," *Journal of Technology and Science Education*, vol. 7, no. 2, pp. 162–171, 2017.

[71] J. E. DeBello, S. Schmeelk, D. M. Dragos, E. Troja, and L. M. Truong, "Teaching effective cybersecurity through escape the classroom paradigm," in *2022 IEEE Global Engineering Education Conference (EDUCON)*, 2022. doi: 10.1109/EDUCON52537.2022.9766684 pp. 17–23.

[72] F. A. Deeb and T. J. Hickey, "Teaching introductory cryptography using a 3d escape-the-room game," in *IEEE Frontiers in Education Conference (FIE)*, Covington, KY, 2019, pp. 1–6.

[73] E. Löffler, B. Schneider, T. Zanwar, and P. M. Asprion, "CySecEscape 2.0—a virtual escape room to raise cybersecurity awareness," *International Journal of Serious Games*, vol. 8, no. 1, p. 59–70, Mar. 2021.

[74] C. C. Taladriz, "Flipped mastery and gamification to teach computer networks in a cybersecurity engineering degree during covid-19," in *2021 IEEE Global Engineering Education Conference (EDUCON)*, 2021. doi: 10.1109/EDUCON46332.2021.9453885 pp. 1624–1629.

[75] T. Williams and O. El-Gayar, "Design of a virtual cybersecurity escape room," in *National Cyber Summit (NCS) Research Track 2021*, vol. 310. Huntsville, AL: NCS, 2021, pp. 1–14.

[76] R. S. Weiss, S. Boesen, J. F. Sullivan, M. E. Locasto, J. Mache, and E. Nilsen, "Teaching cybersecurity analysis skills in the cloud," in *Proceedings of the 46th ACM Technical Symposium on Computer Science Education*, ser. SIGCSE '15. New York, NY, USA: Association for Computing Machinery, 2015. doi: 10.1145/2676723.2677290. ISBN 9781450329668 p. 332–337.

[77] Y. Nerbraten and L. Rostad, "hACMEgame: A tool for teaching software security," in *2009 International Conference on Availability, Reliability and Security*. Fukuoka, Japan: CISIS, 2009. doi: 10.1109/ARES.2009.135 pp. 811–816.

[78] P. Morreale, N. Diplan, and D. York, "A gamification pathway for computer science student success," in *ITiCSE '19: Proceedings of the 2019 ACM Conference on Innovation and Technology in Computer Science Education*. Aberdeen, UK: ACM, 2019. doi: 10.1145/3304221.3325577 p. 317.

[79] 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*, ser. SIGCSE '21. New York, NY, USA: Association for Computing Machinery, 2021. doi: 10.1145/3408877.3432544. ISBN 9781450380621 p. 1135–1141.

[80] T. Chothia and C. Novakovic, "An offline capture the Flag-Style virtual machine and an assessment of its value for cybersecurity education," in *USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*, Washington, D.C., 2015, pp. 1–8.

[81] S. J. Nielson, "PLAYGROUND: preparing students for the cyber battleground," *Computer Science Education*, vol. 26, no. 4. doi: 10.1080/08993408.2016.1271526 pp. 255–276, 2016.

[82] R. Luh, M. Temper, S. Tjoa, S. S., and J. H., "PenQuest: a gamified attacker/defender meta model for cyber security assessment and education," *J Comput Virol Hack Tech*, vol. 16. doi: 10.1007/s11416-019-00342-x pp. 19–61, 2020.

[83] J. Giboney, J. McDonald, and J. Balzotti, "Increasing cybersecurity career interest through playable case studies," *TechTrends*, vol. 65. doi: 10.1007/s11528-021-00585-w pp. 496–510, 2021.

[84] S. O'Connor, S. Hasshu, J. Bielby, S. Colreavy-Donnelly, S. Kuhn, F. Caraffini, and R. Smith, "SCIPS: A serious game using a guidance mechanic to scaffold effective training for cyber security," *Information Sciences*, vol. 580. doi:

10.1016/j.ins.2021.08.098 pp. 524–540, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0020025521009129

[85] S. Koch, J. Schneider, and J. Nordholz, "Disturbed playing: Another kind of educational security games," in *5th Workshop on Cyber Security Experimentation and Test (CSET 12)*. Bellevue, WA: USENIX Association, Aug 2012, pp. 1–9. [Online]. Available: https://www.usenix.org/conference/cset12/workshop-program/presentation/Koch

[86] B. Alothman, A. Alhajraf, R. Alajmi, R. Al Farraj, N. Alshareef, and M. Khan, "Developing a cyber incident exercises model to educate security teams," *Electronics (Switzerland)*, vol. 11, no. 10. doi: 10.3390/electronics11101575 2022.

[87] K. B. Vekaria, P. Calyam, S. Wang, R. Payyavula, M. Rockey, and N. Ahmed, "Cyber range for research-inspired learning of "attack defense by pretense" principle and practice," *IEEE Transactions on Learning Technologies*, vol. 14, no. 3. doi: 10.1109/TLT.2021.3091904 pp. 322–337, 2021.

[88] Naval Postgraduate School, "Incorporating CyberCIEGE into an introductory cyber security course," 2021, accessed: 2022-03-14. [Online]. Available: https://nps.edu/web/c3o/cyberciege

[89] M. Thompson and C. Irvine, "Active learning with the cyberciege video game," in *Proceedings of the 4th Conference on Cyber Security Experimentation and Test*, ser. CSET'11. USA: USENIX Association, 2011, p. 10.

[90] A. Parakh, M. Subramaniam, and E. Ostler, "QuaSim: A virtual quantum cryptography educator," in *IEEE International Conference on Electro Information Technology (EIT)*, 2017, pp. 600–605.

[91] CTF Time Team, "Ctf time," 2021, accessed: 2022-03-14. [Online]. Available: https://ctftime.org/

[92] Order of the Overflow, "Defcon capture the flag qualifier," 2021, accessed: 2022-03-14. [Online]. Available: https://oooverflow.io/

[93] Dark Tangent, "Defcon capture the flag," 2021, accessed: 2022-03-14. [Online]. Available: https://defcon.org/html/links/dc-ctf.html

[94] G. Vigna, "Ucsb international capture the flag," 2021, accessed: 2022-03-14. [Online]. Available: https://shellphish.net/ictf/

[95] N. Backman, "Facilitating a battle between hackers: Computer security outside of the classroom," in *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, ser. SIGCSE '16. New York, NY, USA: Association for Computing Machinery, 2016. doi: 10.1145/2839509.2844648. ISBN 9781450336857 p. 603–608.

[96] M. Carlisle, M. Chiaramonte, and D. Caswell, "Using CTFs for an undergraduate cyber education," in *2015 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 15)*. Washington, D.C.: USENIX Association, Aug 2015, pp. 1–6. [Online]. Available: https://www.usenix.org/conference/3gse15/summit-program/presentation/carlisle

[97] S. Karagiannis and E. Magkos, "Adapting CTF challenges into virtual cybersecurity learning environments," *Information & Computer Security*, vol. 29, no. 1. doi: 10.1108/ICS-04-2019-0050 pp. 105–132, 2021.

[98] J. Vykopal, V. Švábenský, and E.-C. Chang, *Benefits and Pitfalls of Using Capture the Flag Games in University Courses*. New York, NY, USA: Association for Computing Machinery, 2020, p. 752–758. ISBN 9781450367936

[99] ACM-IEEE Joint Task Force on Computing Curricula, "Computer science curricula 2013: Curriculum guidelines for undergraduate degree programs in computer science," 2013. [Online]. Available: https://www.acm.org/binaries/content/assets/education/cs2013_web_final.pdf

[100] G. Ferraro, G. Lagorio, and M. Ribaudo, "Cyberchallenge.it@unige: Ethical hacking for young talents," in *Adjunct Publication of the 28th ACM Conference on User Modeling, Adaptation and Personalization*, ser. UMAP '20 Adjunct. New York, NY, USA: Association for Computing Machinery, 2020. doi: 10.1145/3386392.3399311. ISBN 9781450379502 p. 127–134.

[101] D. Vitorino, I. I. Bittencourt, and G. Chalco, "StarsCTF: A capture the flag experiment to hack player types and flow experience," *Smart Innovation, Systems and Technologies*, vol. 255. doi: 10.1007/978-981-16-4884-7_39 p. 467 – 477, 2022.

[102] M. A. Kornegay, M. T. Arafin, and K. Kornegay, "Engaging underrepresented students in cybersecurity using capture-the-flag(CTF) competitions (experience)," in *ASEE Annual Conference and Exposition, Conference Proceedings*, 2021.

[103] R. Chicone, T. Burton, and J. Huston, "Using facebook's open source capture the flag platform as a hands-on learning and assessment tool for cybersecurity education," *International Journal of Conceptual Structures and Smart Applications (IJCSSA)*, vol. 6, no. 1. doi: 10.4018/IJCSSA.2018010102 p. 15, 2018.

[104] J. Yang, O.-G. Niculaescu, and G. Ghinita, "A game-oriented educational tool for location privacy topics," in *Proceedings of the 25th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*, ser. SIGSPATIAL '17. New York, NY, USA: Association for Computing Machinery, 2017. doi: 10.1145/3139958.3140016. ISBN 9781450354905

[105] D. Antonioli, H. R. Ghaeini, S. Adepu, M. Ochoa, and N. O. Tippenhauer, "Gamifying ics security training and research: Design, implementation, and results of S3," in *Proceedings of the 2017 Workshop on Cyber-Physical Systems Security and PrivaCy*, ser. CPS '17. New York, NY, USA: Association for Computing Machinery, 2017. doi: 10.1145/3140241.3140253. ISBN 9781450353946 p. 93–102.

[106] Z. Romano, J. Windsor, M. VanDerPol, and J. Coffman, "Election security in the cloud: A ctf activity to teach cloud and web security," in *2021 IEEE Frontiers in Education Conference (FIE)*. Lincoln, NE: IEEE, 2021. doi: 10.1109/FIE49875.2021.9637368 pp. 1–5.

[107] M. Lehrfeld and P. Guest, "Building an ethical hacking site for learning and student engagement," in *SoutheastCon 2016*. Norfolk, VA: IEEE, 2016. doi: 10.1109/SECON.2016.7506746 pp. 1–6.

[108] R. Broholm, M. Christensen, and L. T. Sørensen, "Exploring gamification elements to enhance user motivation in a cyber security learning platform through focus group interviews," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2022. doi: 10.1109/EuroSPW55150.2022.00056 pp. 470–476.

[109] Haaukins, "Haaukins," 2022, accessed: 2022-03-14. [Online]. Available: https://general.haaukins.com/

[110] HackTheBox, "HackTheBox," 2022, accessed: 2022-03-14. [Online]. Available: https://hackthebox.com/

[111] picoCTF, "picoCTF," 2022, accessed: 2022-03-14. [Online]. Available: https://picoctf.org/

[112] C. Li, Z. Dong, R. H. Untch, and M. Chasteen, "Engaging computer science students through gamification in an online social network based collaborative learning environment," *International Journal of Information and Education Technology*, vol. 3, no. 1, p. 72, 2013.

[113] A. A. De Freitas and M. M. de Freitas, "Classroom Live: a software-assisted gamification tool," *Computer Science Education*, vol. 23, no. 2, pp. 186–206, 2013.

[114] B. S. Clegg, J. M. Rojas, and G. Fraser, "Teaching software testing concepts using a mutation testing game," in *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET)*. Buenos Aires, Argentina: IEEE/ACM, 2017. doi: 10.1109/ICSE-SEET.2017.1 pp. 33–36.

[115] V. Švábenský, J. Vykopal, M. Cermak, and M. Lastovicka, "Enhancing cybersecurity skills by creating serious games," *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*. doi: 10.1145/3197091.3197123 2018.

[116] S. C. McGregor, Chan, S. Wlodarczyk, and M. Maarek, "Aligning a serious game, secure programming and cybok-linked learning outcomes," in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, 2022. doi: 10.1109/EuroSPW55150.2022.00058 pp. 486–495.

[117] P. Čeleda, J. Vykopal, V. Švábenský, and K. Slavíček, *KYPO4INDUSTRY: A Testbed for Teaching Cybersecurity of Industrial Control Systems*. New York, NY, USA: Association for Computing Machinery, 2020, p. 1026–1032. ISBN 9781450367936

[118] T. Chothia, S. Holdcroft, A.-I. Radu, and R. J. Thomas, "Jail, hero or drug lord? turning a cyber security course into an 11 week choose your own adventure story," in *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, 2017, pp. 1–11.