*Article*

# Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games

Simulation & Gaming
2020, Vol. 51(5) 586–611

DOI: 10.1177/1046878120933312
journals.sagepub.com/home/sag
SAGE

**Merijke Coenraad[1], Anthony Pellicone[1], Diane Jass Ketelhut[1], Michel Cukier[1], Jan Plane[1], and David Weintrop[1]**

## Abstract

*Background.* **Cybersecurity** is of increasing importance in our interconnected world, yet the field has a growing workforce deficit and an underrepresentation of women and people of color. In an effort to address these issues, many digital games have been created to teach individuals about cybersecurity and keeping themselves, their data, and their networks safe.

*Intervention.* We present the results of a **systematic review** of **digital games** related to **cybersecurity** as a means to understand how players are being introduced to cybersecurity in game-based contexts.

*Methods.* Using a systematic search, we identified 181 games related to cybersecurity (either through content or aesthetics) by searching the Apple App Store, the Google Play Store, Steam, and the web broadly. Each game was played for up to an hour and characteristics such as the game story, game elements, and presentation of cybersecurity were gathered.

*Results.* We found diverse conceptualizations of cybersecurity and of cybersecurity professionals. Further, the nature of games and the framing of cybersecurity varied by the platform and device on which the game was available (computer, mobile, or web). Web games were most likely to present cybersecurity as cyber safety and were more likely to be a gamified quiz or worksheet. Computer

[1]University of Maryland, College Park, USA

**Corresponding Author:**
Merijke Coenraad, College of Education, University of Maryland, College Park, 2226 Benjamin Building, College Park, MD 20742, USA.
Email: mcoenraa@umd.edu

and mobile games tended to present cybersecurity through game aesthetics or deep content engagement. The games mirrored the underrepresentation of women and minoritized individuals in the field.

*Discussion.* With the variety of digital cybersecurity games and the differences in games based on the platform on which the game is available, it is important game developers move beyond presenting cybersecurity through gamification and focusing on cyber safety. The current scope of cybersecurity games leaves room for the development of games focused on deeper content engagement with cybersecurity topics in an environment conducive to the broadening participation goals of the cybersecurity field.

**Keywords**
cybersecurity, digital game-based learning, digital games

## Introduction

Given the increasing number of cyber-attacks, more cyber professionals are needed (Symantec Corp., 2018). However, there exists a shortage of qualified individuals. It is expected that by 2022, 1.8 million cybersecurity jobs globally will be unfilled due to a lack of qualified candidates (Center for Cyber Safety and Education, 2017). To develop innovative solutions and foster new ideas, the field of cybersecurity needs not only more candidates, but a diverse range of candidates (Turner, 2009; Yang & Konrad, 2011). In the United States, only 14% of the cybersecurity field identifies as a race underrepresented in computing (African American or Black, Hispanic, American Indian or Alaskan Native, or Native Hawaiian/Pacific Islander), and only 14% of the field identifies as a woman (Reed & Acosta-Rubio, 2017). Given the importance of a diverse workforce to address the security challenges to come, the field of cybersecurity must recruit not only more, but more diverse, individuals to grow and thrive. For the purposes of this review we are focusing on the Association for Computing Machinery's (Burley et al., 2017) working definition of cybersecurity as an academic curriculum,

> "A computing-based discipline involving technology, people, information, and processes to enable assured operations. It involves the creation, operation, analysis, and testing of secure computer systems. It is an interdisciplinary course of study, including aspects of law, policy, human factors, ethics, and risk management in the context of adversaries" (p. 1).

Conventionally, cybersecurity is taught in upper-level undergraduate computer science courses to students who have already learned the fundamentals of computer science and have demonstrated a commitment to computing careers (Dark, 2002; Svabensky et al., 2020). Practically, the effect of the undergraduate bottleneck to formal cybersecurity learning is exacerbated by existing inequities in the K-12 pipeline for computer science as a broader field (Shumba et al., 2013). Cybersecurity programs for high school-aged learners (e.g. GenCyber; Ladabouche & LaFountain, 2016) are being designed to introduce security concepts to students at younger ages and build interest

(Bashir et al., 2015). These initiatives have been successful in increasing interest early on, but more can be done to spread cybersecurity knowledge to the general public and increase interest in the adoption of cybersecurity practices and working in the field (Wee et al., 2016).

One method for increasing public awareness that can help to build the skills of the general public and catch the attention of future cybersecurity professionals is digital games (henceforth referred to simply as 'games,' with the caveat that we are only considering digital formats in this review). Playing games is a widespread activity across race, gender and socioeconomic status (Duggan, 2015; Juul, 2010). Games have a number of features that enable them to serve as powerful contexts for informal learning (Gee, 2004, 2007) One of the most powerful affordances of games is their ability to help players develop identities within the content areas that games are set (Squire, 2006), and their role as a testing ground for new identities (Konijn & Bijvank, 2009).

In our research, we aim to better understand the current landscape of cybersecurity games and the ways in which cybersecurity is presented through games that appear to be related to or label themselves as cybersecurity. We conducted a systematic review of games available through the web, mobile app stores, and Steam. We focus on how games present cybersecurity to better understand the cybersecurity content being disseminated to the public through games and how cybersecurity is represented. Further, we analyze games for issues related to racial and gender inclusiveness to see if and how the games may advance the goal of broadening participation in cybersecurity careers. Without offering extensive positive or negative evaluation of the currently available games, we hope to provide an overview of current games to guide the work of designers aiming to create new cybersecurity games. Specifically, this work seeks to answer the following research questions:

1. What cybersecurity content is being conveyed through digital games and what cybersecurity practices are promoted?
2. How are cybersecurity professionals presented in digital games?

## Background

### *Game-based Learning as a Pathway for Underrepresented Learners Towards Cybersecurity*

Game-based learning has emerged as an important strategy for engaging youth in learning experiences outside of formal settings. Widescale meta studies have found that games are effective in terms of teaching skills through active engagement (Clark et al., 2016), and by motivating and inspiring affective connections to content (Connolly et al., 2012). These findings regarding the effectiveness of games as learning environments bear out earlier theoretical work about the design of commercial games as learning environments, and the potential of games designed expressly for the purpose of education. Gee (2004, 2007) theorized that well-designed games can engage learners who might otherwise not see their identities as being represented in traditional

classroom instruction. The type of experiential learning offered through games provides an avenue to engage players with domains and concepts that might not be readily available through traditional classroom methods through the affordances and literacies of digital gameplay (Gee, 2005).

Squire (2006) argued that games are 'designed experiences', and that "In videogames, knowing is at its essence a kind of performance, as learners learn by doing . . . The focus is on experience that enables students to develop situated understandings, to learn through failure, and to develop identities as expert problem solvers" (p. 26). The experiences that Squire refers to above can serve as powerful educational environments that can help to bridge differences between students who are entering a learning environment with already high self-efficacy, versus students who experience low self-efficacy in that domain (Ketelhut, 2007). Effective application of games in learning is centered on the way that the game interacts with a learner's individual history and relationship to a domain, the affordances of the game itself, and the contexts in which the player is encountering the game (Squire & Jenkins, 2011). Even in commercial games not designed specifically for educational contexts, the socially situated practice of a player incorporating a game into their reality is powerful form of learning through play (Calleja, 2011; Iacovides et al., 2014). However, research suggests that there is a balance in game-based learning between giving players space to play with a domain or a concept, and deep content engagement that allows the player to apprehend and make use of concepts outside the realm of play (Clark et al., 2014; Holbert & Wilensky, 2019).

Playful experiences like hackathons and capture the flag events are a common interest building tool for cybersecurity (Ricci & Gulick, 2017). These experiences can serve to increase interest in the discipline through active with real cybersecurity tools and practices (Jin et al., 2018; Svabensky & Vykopal, 2018). However, these events have trouble attracting populations that do not mirror the existing cybersecurity workforce (Tobey et al., 2014).

Since play and games have a history within cybersecurity as a means of recruiting and exciting young learners (Pusey et al., 2016), and since game-based learning is broadly effective at introducing learners to unfamiliar domains where they may not have much traditional representation (Ketelhut, 2007), this work seeks to understand the current landscape of cybersecurity games available to youth.

## Methods

In this game review, we used systematic searches of common game repositories to identify games related to cybersecurity currently available to the general public. We are using an intentionally broad definition of cybersecurity to include not only content but also graphical representations and narrative conceits. The broadness of the selection process was intentional given our stated goals of understanding how cybersecurity (as a broader discipline) is being portrayed in games, and in analyzing the depiction of cybersecurity professionals. We collected and analyzed each game to understand the

nature of cybersecurity content, the context in which the content was situated, the roles and identities players take on when playing, and the technical and design aspects.

### *Game Identification and Collection*

To develop our list of candidate cybersecurity games, we searched four different venues: Steam, the Google Play Store, the Apple App Store, and the Internet using the Google search engine. These venues were selected as leading locations where consumers find games. Each platform was searched using the same search terms: *cybersecurity game*, *cyber game*, and *security game*. To maintain systematicity, as similar a search process as possible was followed on each platform. We focused specifically on games available in English. This methodological choice was motivated by two considerations: the capacity of the research team, which found English the most accessible language to conduct our analysis; and our focus on Cybersecurity specifically from the perspective of what young players in the United States would experience as they are coming through the cybersecurity career pipeline. Since our selection methodology involved open search engines, we are operating under the assumption that if a game appeared in our search results then it is generally available within the United States.

To be included in the review, games needed to be fully digital (i.e., no physical components), available to the general public (i.e., not for specific companies or purchased through a company membership), available in English, playable through a computer or mobile device, and presented in a cybersecurity context. Games were considered to be in a cybersecurity context if they conveyed cybersecurity content, mentioned cybersecurity, or were set in a cyber environment such as inside a computer or the internet. Games were not included if results led to commercial game pages (i.e., Yahoo games or AOL games) rather than specific cyber-related games, the game was only available with virtual reality, or if the game or app was an add-on to an existing game. If both a free and paid version of a game were available, the free version was used. For games where a free version was not available, the paid version was purchased.

For the Google searches, every link on the first ten pages (the top 100 results) was opened and examined to determine if the link led to a cybersecurity game. After ten pages, up to the next fifteen pages were skimmed by reading titles and the information in the search results. Google searches were terminated when five pages in a row resulted in no new games or results ended. If a website lead to multiple cybersecurity games, all games were included in the review. For mobile app stores and the Steam store, all search results were considered with the first 100 results being fully examined and the rest skimmed for relevancy.

The search was conducted in the fall of 2018 and resulted in an initial list of 214 games. During game play, which took place between the fall 2018 and summer 2019, 33 games were removed for not meeting the criteria described above. A total of 181 games were included in the final analysis (see Figure 1; Supplementary Appendix).

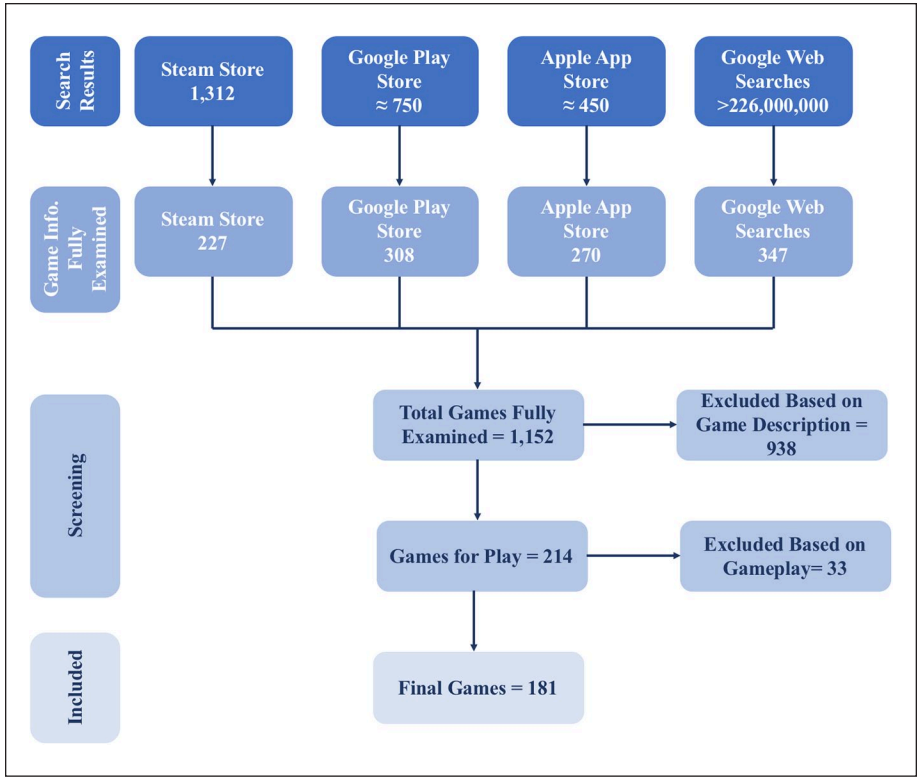


**Figure 1.** Game identification and review process.
*Source*: Adapted from Liberati et al. (2009, p. 4).
*Note*. Approximate search results reported for Google Play Store and Apple App Store because platforms do not provide search totals.

## *Game Play and Data Collection*

Each game was played by the same researcher according to a set protocol. Story-based games were played for a maximum of one hour in a single sitting. Points-based arcade games in which the levels changed but mechanics and knowledge did not differ between levels were played for a maximum of 30 minutes in a single sitting. Following game play, information was collected about each game using the categories of analysis developed by Clark et al. (2016), as well as added categories pertaining to racial and gender diversity and cybersecurity topics and a summary of the game (see Table 1). The categories from Clark et al. (2016) were used as they reflect a comprehensive and well-established set of dimensions upon which to evaluate a game. Further, Clark et al. (2016) generated these criteria from other existing meta-reviews (Sitzmann, 2011; Vogel et al., 2006; Wouters et al., 2013), so they represent a set of factors to be

**Table 1.** Data Collection Categories.

| | | |
|---|---|---|
| **Game Basics** | | |
| Game Name | Link and Source | Company/Agency of Ownership |
| Publication Date | Price | Target Audience |
| Play Time | Number of Sessions* | |
| **Story** | | |
| Game Story/Summary | Game Story Motivation | Story Relevance* |
| Story Depth* | | |
| **Educational/Cybersecurity Content** | | |
| Cybersecurity Concepts Covered (mentioned or defined) | Non-Cybersecurity Concepts Covered | Framing of Cybersecurity |
| **Player/Characters** | | |
| Player Role | Gender of Characters | Role of Women |
| Race of Characters | Anthropomorphism* | |
| **Game Mechanics** | | |
| Game Type* | Variety of Game Actions* | Intrinsic/Extrinsic Type* |
| Scaffolding* | Visual Realism* | Camera View* |

*Note*. Categories marked with an asterisk (*) were developed by Clark et. al (2016).

considered when reviewing educational games. Game-specific data such as name, source, ownership, and price were collected as published on the game website or store. Data collection under the categories developed by Clark et al. (2016) was performed using the set parameters developed in their meta-analysis.

To assure reliability of the gathered results, a second researcher played 10% of the games (18 in total) following the same coding procedure as the main researcher. The 18 games were selected randomly from the larger game selection and the game list was examined before second coding began to ensure that all gaming platforms (computer, web, and mobile) were included in the second coding. Interrater reliability for all categorically gathered dimensions was calculated using Cohen's Kappa and was found to be within the substantial agreement range ($\kappa$=0.73, $z = 15.7$, $p<0.001$; Landis & Koch, 1977).

## *Data Analysis*

Data collected in narrative form were coded using open coding to create inductive categories. Multiple researchers met to discuss the categories and decide on the final list. Then, the main researcher who played the games coded the narratives using descriptive coding and the developed categories (Saldaña, 2015). Once all data had been categorized and could be quantified, counts were generated for each category and basic statistics were calculated.

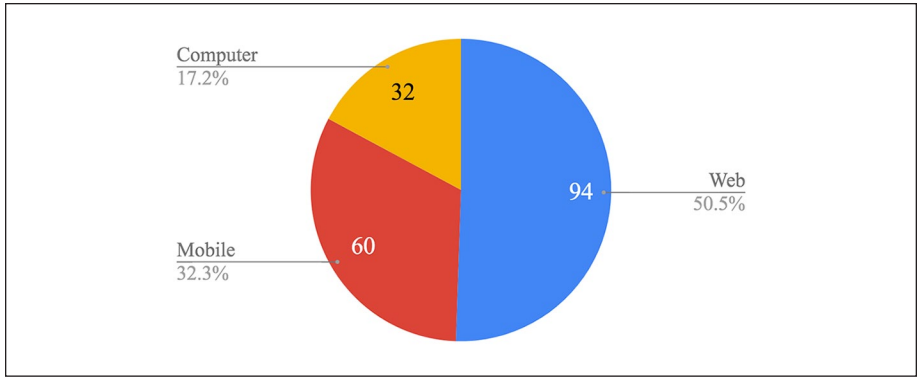


**Figure 2.** Games by platform.

## Results

In the following section, we present the results of our game review. We focus on presenting an overview of the games through a characterization of what is available, summary of how cybersecurity is portrayed within games, and discussion of the representation of cybersecurity professionals within the games. Through these results, we aim to highlight the current landscape of cybersecurity games through a presentation of what is currently available.

### *Characterization of Games*

*Game development.* Of the 181 games played for this review, 94 were available on the web, 32 were available in a downloadable computer format, and 60 were available on mobile devices (32 Android, 34 for iOS devices, including 6 on both platforms) (see Figure 2). Games were developed by creators in six categories: for-profit non-gaming companies (e.g., cybersecurity firms, technology companies), game companies, nonprofit companies, government agencies, academic institutions, and individuals (see Figure 3). Game development differed by platform.

Based on available information, we examined the country in which the developing company or individual was based. Such information was found for 86.7% of the games. The cybersecurity games within this review were developed on all six inhabited continents with the majority of games developed in North America (42.0%) and Europe (28.7%), but not all games were developed in English dominant countries. Fourteen games (7.7%) were developed in Asia, 12 (6.6%) were developed in Oceania, 2 (1.1%) were developed in South America, and 1 (0.55%) was developed in Africa.

*Audience.* Based on content, 34 (18.7%) games are targeted toward players beginning in elementary school, 53 (29.3%) games for players beginning in middle school, and 94 (51.9%) games for players beginning in high school. While some of the games

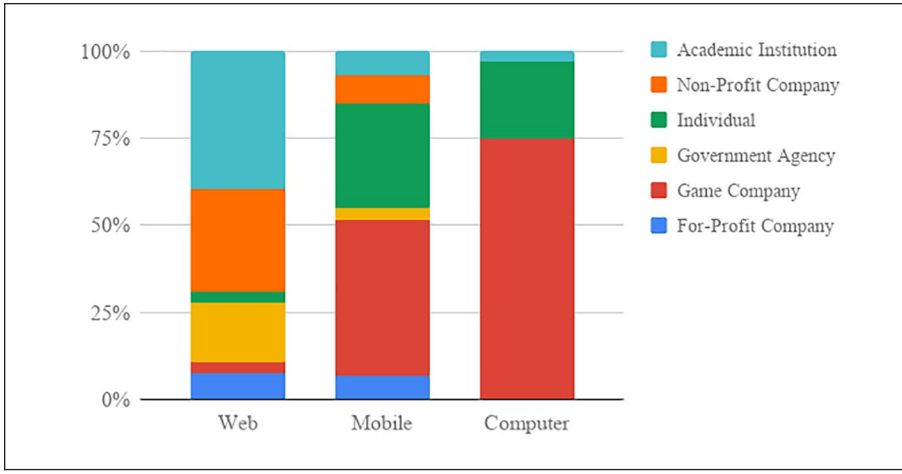


**Figure 3.** Game developers.

**Table 2.** Play Time for Games by Platform.

| Platform | Single Session (< 1 hour total play) Games | Multiple Session (> 1 hour total play) Games | Average Playtime in Minutes |
|---|---|---|---|
| Web | 88 | 6 | 14.31 (*SD*=19.00) |
| Mobile | 14 | 46 | 37.72 (*SD*=22.79) |
| Computer | 0 | 32 | 52.5 (*SD*=20.97) |
| Total | 100 | 81 | 28.07 (*SD*=22.75) |

would likely only be interesting to elementary or middle school players because of ease, graphics, and characters, the majority of games would be appropriate for high school aged players and beyond (14 years old and beyond), making them the largest served population by cybersecurity games.

*Play time.* On average, games were played for 28 minutes ($SD = 22.75$, Range = 59), with play length differing by platform (see Table 2). Computer games were played for the longest time, while web games were played for the shortest time.

*Visual realism.* Cybersecurity content was presented mostly through cartoon graphics (71.3%; see Figure 4a), but was also represented through schematics (26.0%; see Figure 4b) and realistic images (2.8%; see Figure 4c; Table 3).

*Camera view.* The majority of games took either a first person (46.1%) or third person (43.1%) point of view, either providing a vantage point through the players eyes or through a static view that was non-camera-based (see Table 3).


**Figure 4.** Visual realism in cybersecurity games. (a) Cartoon graphics. *Source*: Reproduced with permission from Life Education Australia (2018), (b) Schematics. *Source*: Reproduced with permission from i273 LLC (2016), (c) Realistic Images. *Source*: Reproduced with permission from Texas A&M Division of Information Technology (2017).

**Table 3.** Visual Realism, Camera View, and Anthropomorphism in Cybersecurity Games.

| Game Characteristic | Game Count | Percentage |
|---|---|---|
| Visual Realism | | |
| Cartoon | 129 | 71.3% |
| Schematic | 47 | 26.0% |
| Realistic | 5 | 2.8% |
| Camera View | | |
| First Person | 84 | 46.4% |
| Over the Shoulder/Overhead Tracking | 19 | 10.5% |
| Third Person | 78 | 43.1% |
| Anthropomorphism | | |
| Low/None | 149 | 82.3% |
| Medium | 11 | 6.1% |
| High | 21 | 11.6% |

*Anthropomorphism.* While anthropomorphism was present within the cybersecurity games examined in this review, it was used to an extent that was equal or more prevalent than non-anthropomorphic entities in only 17.7% of games (see Table 3).

## *RQ 1: What Cybersecurity Content Is Being Conveyed Through Digital Games and What Cybersecurity Practices Are Promoted?*

*Game story.* The examined games typically included a game story to motivate the cybersecurity content and tie the game together. Yet, oftentimes the story lacked details and was irrelevant to the actions being performed (see Table 4). An example of a relevant story can be seen in the game Mainlining (Rebelephant, 2017) where players work for a government agency to stop a cyber-criminal network by *hacking* to investigate and bring criminals to justice. Alternately, Catch the Software Bugs

**Table 4.** Story Elements in Games.

| Platform | Has a Story | Relevant Story | Thin Story Depth | Medium Story Depth | Thick Story Depth |
|---|---|---|---|---|---|
| Web | 66 (70.2% of games) | 45 (68.2% of stories) | 49 (52.1% of games) | 14 (14.9% of games) | 3 (3.2% of games) |
| Mobile | 43 (71.7% of games) | 31 (72.1% of stories) | 22 (36.7% of games) | 11 (18.3% of games) | 10 (16.7% of games) |
| Computer | 30 (93.8% of games) | 20 (66.7% of stories) | 5 (15.6% of games) | 12 (37.5% of games) | 13 (40.6% of games) |
| Total | 134 (74.0% of games) | 94 (70.2% of stories) | 75 (41.4% of games) | 33 (18.2% of games) | 26 (14.4% of games) |

(Carnegie Mellon University, 2019) has an irrelevant story. In this game, players are trying to get rid of computer bugs, represented as beetles crawling around a computer chip, using a fly swatter.

Game stories were categorized according to their depth as either thin, medium, or thick (see Table 4). A thin story only gives a cybersecurity setting or context. For example, in the game Data Jammers: FastForward (Digital Eel, 2011), players are a data packet moving through cyberspace trying to get into a system to take it down. Medium story depth includes some emerging story within the game, such as in the game Cyber Lab (WGBH Educational Foundation, 2014). In this game, players are a security specialist at a new social media company and have to address a series of security threats to help launch the site. While the game has a partial storyline, the story does not deepen as the game evolves. Finally, thick storylines have a rich and evolving story throughout game play. In the game Orwell: Keeping an Eye on You (Osmotic Studios, 2016), players take on the role of a new agent using the Orwell platform. The player must figure out who is responsible for a terrorist attack by listening to the suspect's conversations and gathering facts from news articles, blogs, and other websites. As gameplay moves forward, new information is provided to the player.

*Game actions.* Aligning with the story findings, the games examined in this review tended to be simplistic, emphasizing the collection of points or badges over more complex actions such as solving puzzles, using command line coding to follow stories, or piecing together a storyline (114 games; 63.0%; Table 5).

Games varied in the variety and complexity of actions players could perform. Games with a small variety of game actions require players to click on answers or perform just one or two actions, such as dragging or typing. Medium game actions allow players to interact with their environments in multiple ways and explore the overall environment. Finally, a large variety of game actions means players interact with environments in many different ways. The smallest number of required actions were in web games and the largest were in computer games (see Table 5).

**Table 5.** Game Actions by Platform.

| Platform | Adding Points/ Badges | More than Adding Points/Badges | Small Variety of Game Actions | Medium Variety of Game Actions | Large Variety of Game Actions |
|---|---|---|---|---|---|
| Web | 80 (85%) | 14 (15%) | 81 (86%) | 11 (12%) | 2 (2%) |
| Mobile | 30 (50%) | 30 (50%) | 36 (60%) | 21 (35%) | 3 (5%) |
| Computer | 7 (22%) | 25 (78%) | 8 (25%) | 14 (44%) | 10 (31%) |
| Total | 114 (63%) | 67 (37%) | 122 (67%) | 45 (25%) | 14 (8%) |

**Table 6.** Game Actions by Story Depth.

| Story Depth | Adding Points/ Badges | More than Adding Points/ Badges | Small Variety of Game Actions | Medium Variety of Game Actions | Large Variety of Game Actions |
|---|---|---|---|---|---|
| Thin | 59 (78.7%) | 16 (21.3%) | 55 (73.3%) | 16 (21.3%) | 4 (5.3%) |
| Medium | 13 (39.4%) | 20 (60.6%) | 14 (42.4%) | 16 (48.5%) | 3 (9.1%) |
| Thick | 1 (3.8%) | 25 (96.2%) | 10 (38.5%) | 9 (34.6%) | 7 (26.9%) |

We examined the interactions between game action and story depth (see Table 6). We found thin stories were most likely to award players points or badges rather than have more complex outcomes (78.7% of thin storied games), and medium and thick stories tended to lead to outcomes more complex than points or badges (60.6% of medium storied games and 96.2% of thick storied games). This pattern was echoed in the variety of game actions that players could take. Thin stories were most likely to have a small number of actions available to players (73.3% of thin storied games). Medium stories tended to allow either a small or medium number of game actions (42.4% of medium storied games and 48.5% of medium storied games, respectively). Finally, thick storied games showed a fairly even split of game actions.

The games provided scaffolding in two ways: through experiences of success and failure where points were awarded (75.7%) or by displaying the correct answer for the players (24.3%). Although, when correct answers were displayed, players were often given some explanation of correctness or connection to the story.

*Presentation of cybersecurity content.* Cybersecurity content was presented in three main ways: deep content engagement, cyber safety, and aesthetics (see Figure 5). Games that deeply engage players with cybersecurity content present cybersecurity topics in a meaningful way through gameplay. To fall into this distinction, games need to either be concerned with advanced cybersecurity topics such as networking or encryption or get into the *how* or *why* of cybersecurity concepts. For example, in Firewall Administration (Tulip Project, n.d.) players are given missions by a boss and must fix the firewall code to allow different types of files through. Overall, 35.9% of the games deeply engaged players with cybersecurity content. Most commonly, deep

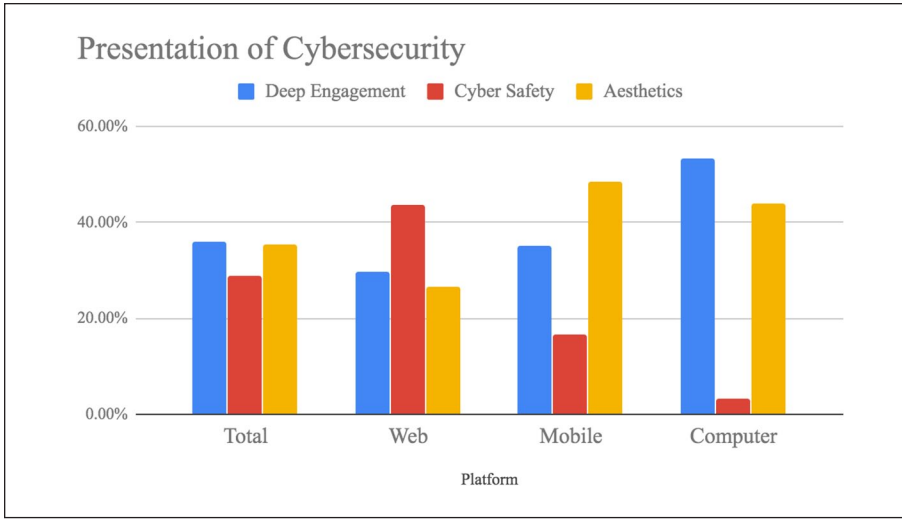


**Figure 5.** Characterizations of cybersecurity.

content engagement games on the computer placed the player in the role of a hacker and required the use of command-line coding to work through computer systems to discover, steal, or delete information.

Another common presentation of cybersecurity was through the idea of cyber safety. Cyber safety refers to what people do to protect against bad actors who might want to steal their private data or use technology to cause harm. These games concentrate on the formation of good cyber habits, such as strong passwords and updating anti-virus software, and support proper online behavior preventing cyberbullying and promoting netiquette. This is seen in the game Interland (Google, n.d.), where players move through four lands performing skills, including spreading kindness online by blocking and reporting bullies, sharing information online, and creating good passwords. Cybersecurity was presented as cyber safety in 28.7% of games but varied drastically depending on the game platform. While 43.6% of games available on the web focused on cyber safety, only 16.7% of mobile games and 3.1% of computer games had this focus.

Another means of presenting cybersecurity is aesthetics (meaning the graphical assets that comprise a game's visual style). In these games, cybersecurity information is not presented; instead, cybersecurity terms or settings are used in games with other purposes. For example, in Obio (Clinkenbeard, 2018), players need to get the Obio bots to upload points by navigating their way through different mazes. As the bots move around the maze, they need to stay away from "virus" blocks and get past "firewalls." In this game, players do not learn cybersecurity content, but the game uses vocabulary and settings that connect to cybersecurity. Aesthetics were used as the frame in 35.4% of games reviewed and was most common on the mobile (48.3%) and computer (43.8%) platforms.

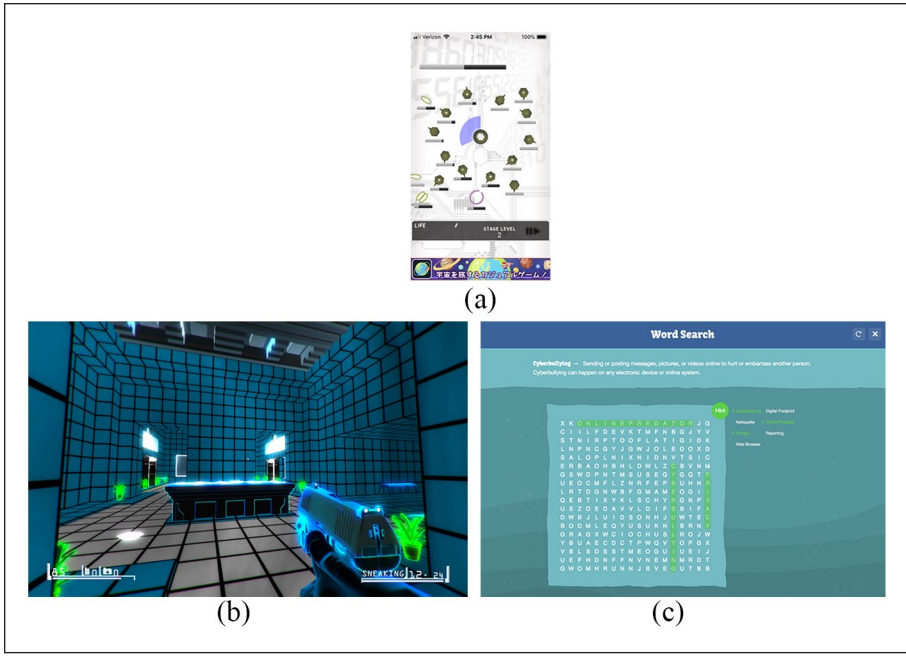


**Figure 6.** Game aesthetics. (a) Cyber-based arcade games. *Source*: Reproduced with permission from AMGAMES Inc. (n.d.), (b) Shooter games. *Source*: Reproduced with permission from Skunkape Interactive (2015), (c) Cybersecurity Terms. *Source*: Reproduced with permission from the Federal Bureau of Investigation (n.d.).

Aesthetics were used in four main ways (see Figure 6). The first was by setting a game in cyberspace or in a location that resembles cyberspace without explicitly covering cybersecurity topics and instead teaching other material. For example, multiple games were connected to the PBS Kids television show Cyberchase, a mathematics learning-centered show that takes place in cyberspace with a group of kids coming into cyberspace to help Motherboard defeat Hacker (Thirteen Productions LLC, 2019). While the games connected to this show take place in cyber contexts and use cybersecurity-related terminology, they focus on teaching problem-solving and math over cybersecurity content. Cybersecurity contexts were also used aesthetically to situate arcade games (see Figure 6a). For example, multiple games used the towers motif, protecting your home base by adding defenses and protecting against waves of attackers, with the defenses named after firewalls and other technological defenses and the attackers taking the form of viruses, worms, and trojan horses. In this style of game, cybersecurity is alluded to through the game story, but it is not the point of the game. Similarly, cyber contexts and stories were used in shooter games available on the computer platform (see Figure 6b). These games were motivated by catching hackers or

**Table 7.** Cybersecurity Content Sharing.

| Integration Method | Total | By Platform | By Developer |
|---|---|---|---|
| Gamified Quiz | 43 (23.8%) | Web - 38 (40.4%)<br>Mobile - 7 (11.7%)<br>Computer - 0 (0.0%) | For-Profit Company - 3 (27.3%)<br>Game Company - 2 (3.8%)<br>Government Agency - 13 (72.2%)<br>Individual - 2 (7.7%)<br>Non-Profit Company - 6 (18.2%)<br>Academic Institution - 17 (43.6%) |
| Gamified Worksheet | 19 (10.5%) | Web - 16 (17.0%)<br>Mobile - 5 (8.3%)<br>Computer - 0 (0.0%) | For-Profit Company - 1 (9.1%)<br>Game Company - 1 (1.9%)<br>Government Agency - 3 (16.7%)<br>Individual - 2 (7.7%)<br>Non-Profit Company - 3 (9.1%)<br>Academic Institution - 9 (22.5%) |
| Arcade Games | 26 (14.4%) | Web - 7 (7.5%)<br>Mobile - 15 (25.0%)<br>Computer 6 - (18.8%) | For-Profit Company - 3 (27.3%)<br>Game Company - 10 (18.9%)<br>Government Agency - 1 (5.6%)<br>Individual - 8 (30.8%)<br>Non-Profit Company - 0 (0.0%)<br>Academic Institution - 4 (10.0%) |
| Puzzle Games | 23 (12.7%) | Web - 12 (12.8%)<br>Mobile - 9 (15.0%)<br>Computer - 3 (9.4%) | For-Profit Company - 0 (0.0%)<br>Game Company - 5 (9.4%)<br>Government Agency - 1 (5.6%)<br>Individual - 5 (19.2%)<br>Non-Profit Company - 8 (24.2%)<br>Academic Institution - 4 (10.0%) |

using hacking skills to get into buildings, but took the form of a typical shooter game. Finally, cybersecurity terms were used in games as answers without much context or description of the terms (i.e., answers to a crossword or word search) (see Figure 6c). The terms used did not impact the game nor provide the player with more information or motivation toward learning cybersecurity.

There are a variety of different methods through which this cybersecurity content was shared and utilized within games (see Table 7). One of the most common types of game utilized for cybersecurity is a gamified quiz. These games integrate cybersecurity content, but typically present it in the form of multiple-choice questions (see Figures 7a). While 23.8% of games examined were gamified quizzes, the likelihood of a game being a gamified quiz differed by platform and developer. Web games (40.4%) and those developed by both government agencies (72.2%) and universities (43.6%) were likely to take the form of gamified quizzes. Another common game type was a gamified worksheet, such as an electronic crossword puzzle, matching worksheet, or word search (see Figure 7b). Gamified worksheets followed many of the same trends as gamified quizzes, with 10.5% of games overall and web games (17,0%) and those created by government agencies (16.7%) and universities (23.1%) being gamified

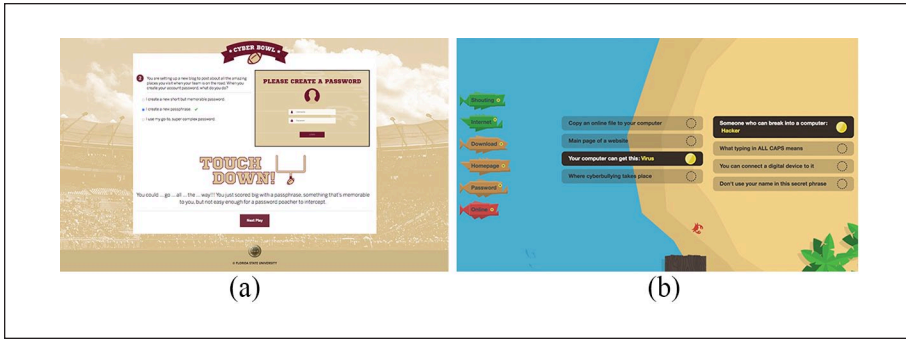


**Figure 7.** Examples of quiz- and worksheet-based cybersecurity games. (a) Gamified Quiz. *Source*: Reproduced with permission from Florida State University Information Technology Services (2018), (b) Gamified Matching Worksheet. *Source*: Reproduced with permission from the Federal Bureau of Investigation (n.d.).

worksheets. Arcade games, those involving some sort of twitch response from the user, made up 14.4% of total games, while puzzle games made up 12.7% of the total games examined and typically included ciphers and decoding.

## *RQ 2: How Are Cybersecurity Professionals Presented in Digital Games?*

While the currently available cybersecurity games present a variety of representations of cybersecurity professionals, the games largely reinforced the current demographics and stereotypes of the cybersecurity workforce as being largely white and male-dominated. In total, 49.2% of games included a gender-defined character, with 2.2% of games allowing players to choose between characters with different gender representations, and 7.7% including characters with an undefined gender (such as being named "Alex") without being shown visually (see Figure 8). Of the games with gender-defined characters, 48.3% represented men and women equally in the game. However, 19.1% of games with gender-defined characters included only males, and 10.1% included women only in a secondary role, such as a secretary. In contrast, 21.4% of games with gender-defined characters showed women in the main role. These overall trends varied according to the platform on which the game was available and the game creator. Gendered web games were more likely to include women than both mobile and computer games (81.1%, 60.9%, and 56.5% respectively). Gendered games created by individuals and government agencies were most likely to include women (100.0% and 90.0%, respectively) and gendered games created by for profit and non-profit companies were the least likely to include female characters (66.7% and 68.8%, respectively).

The race of the characters within cybersecurity games is skewed heavily toward the dominant population and current demographics within the cybersecurity workforce.

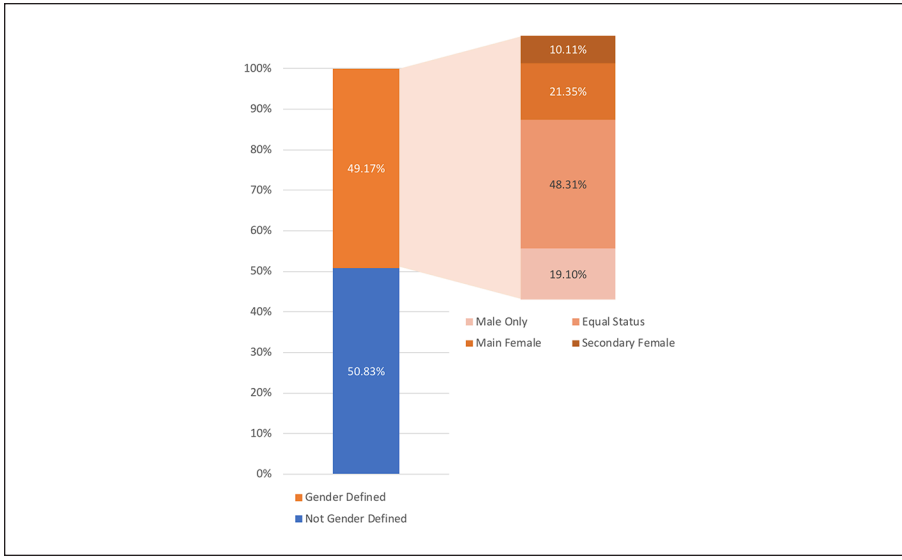


**Figure 8.** Gender in cybersecurity games.

While only 34.3% of games included a visible character, 45.2% of those games included only white characters, and just 8.1% included only characters of minoritized[1] races (see Figure 9). An additional 4.8% of these games allowed the player to choose the race of their character. Although the remaining 41.9% of games with visible characters included characters of multiple races, this does not necessarily equate to equal stature for those characters. Further, games depicting a racial character of color are almost ten times more likely to be web games than they are to be either mobile or computer games (40.3% of web games as compared to 4.8% of each mobile and computer games). Of the games depicting a minoritized character in any way, 80.7% are web games.

Players are presented with a motivation to use cybersecurity both to attack (38.1%) and to defend (61.9%) (see Figure 10). More specifically, players attack both with malicious intent (20.4%) and to protect (11.6%). Additionally, 12.7% of games relate to the social internet where attacking and defending refers to cyberbullying and netiquette. Web games were much more likely to have players motivated by defense (89.4%). Mobile games used the motivations almost equally, with a slight tendency toward attacking (55.0%). Finally, computer games had a strong tendency to motivate players with attacking (90.6%).

## Discussion

In the same way that others have expanded knowledge of climate change games (Reckien & Eisenack, 2013), digital games in sustainable development (Katsaliaki & Mustafee, 2015), and business management simulations (Lopes et al., 2013), the goal

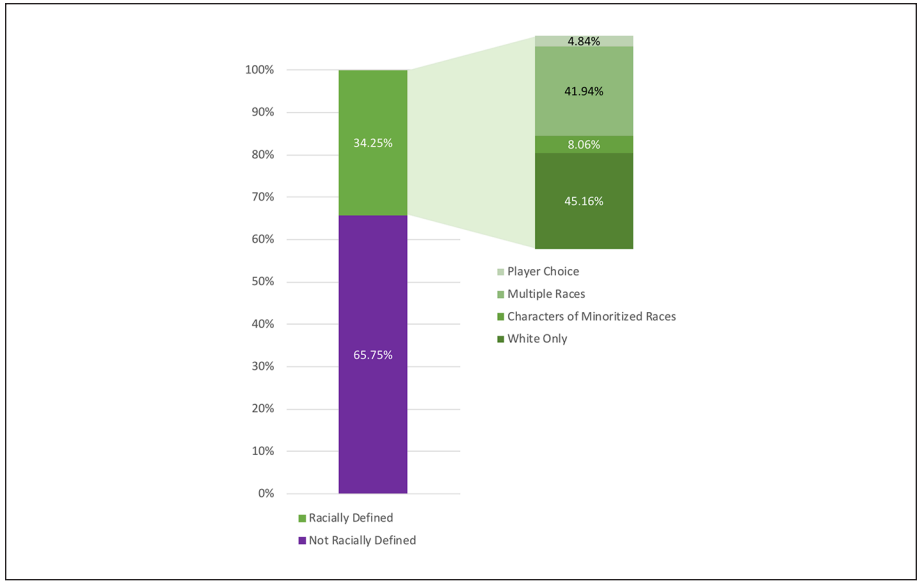


**Figure 9.** Race in cybersecurity games.

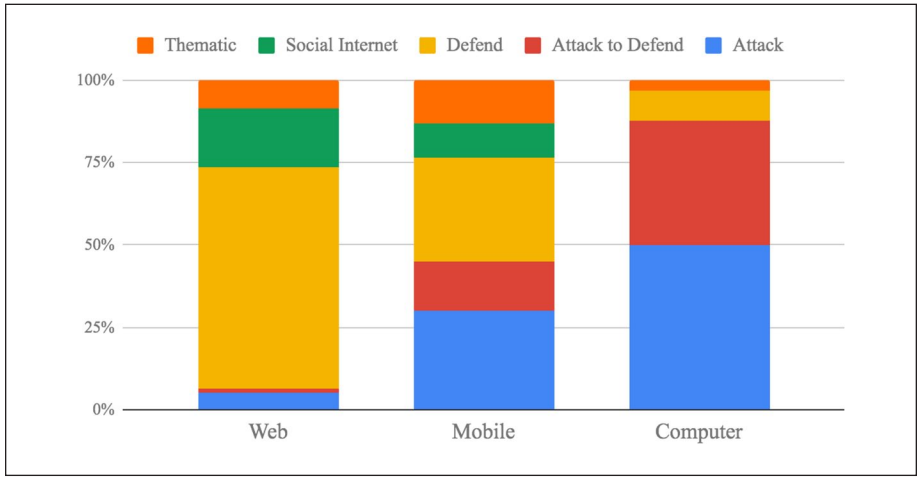


**Figure 10.** Character motivations in cybersecurity games.

of this work is to understand how and where cybersecurity content is present in the current gaming landscape. In this work, we have presented the current landscape of cybersecurity games to highlight the ways cybersecurity is presented through games that appear to be or label themselves as relating to cybersecurity. Through this review we

aim to provide game developers and researchers currently working on cybersecurity games with information about what is currently available to diversify the cybersecurity landscape and identify gaps within the landscape, which others might seek to fill.

The categorization we developed aligns with previous findings of Gestwicki and Stumbaugh (2015) who arrived at a similar taxonomy related to game depth from their more constrained review of games. Our choice to expand our game selection to cover games with both explicit cybersecurity content and aesthetics and narratives related to cybersecurity was informed by our theoretical focus on games as informal avenues to identity development in academic disciplines (Squire, 2006), and the power of commercial games to orient players towards ways of viewing the world and systems of knowledge (Calleja, 2011). Forwarding that exposure to cybersecurity as a more general topic, beyond intentional incorporation into game content, is especially important given the persistent bottleneck of underrepresented learners in pursuing cybersecurity. In the following section we discuss the impacts of our findings and future directions for the development of cybersecurity game-based learning.

## *The Impact of Platform on Game Characteristics and Audience*

In our review of the 181 currently available cybersecurity games, we found differences based on the platform in which the games were hosted (i.e. web, mobile devices, downloadable computer format). Since different groups of people utilize each platform and look for games in different areas depending on availability and interest, this difference by platform can have a significant effect on which types of games are being played by each population and, therefore, the information that each population receives about cybersecurity (Duggan, 2015; Juul, 2010). Web-based games were preferred by government agencies, non-profit companies, and academic institutions. These games were offered free of charge and were quick to play. An online game rarely took a full hour to play, and just six of the online games would require multiple sessions to complete. Through analysis of game mechanics (see Table 1) we found that web games were much more likely to be a gamified quiz or worksheet as compared to other platforms and tended to have thin stories and rely on cartoon graphics and third person point of view. These characteristics point to most web games as attempts to use the notion that games are fun and to use interest in games because of their entertainment value to draw attention to and pass on cybersecurity information. The cybersecurity information presented within web-based games was motivated by defense rather than attacking and tended to be more socially focused, with less inclusion of advanced cybersecurity topics.

Computer games represent the opposite end of the spectrum. Downloadable computer games tended to be created by development companies and individuals, were the most expensive of the games, and took the longest to complete. Computer games were strongly presented with a motivation to attack rather than defend. More than other platforms, computer games presented cybersecurity within a thick story that built during gameplay and allowed the player to perform a large variety of game actions.

Mobile games tended to fall between web-based and computer-based games. Mobile games were either free or purchased for a modest price and were more likely to take multiple sessions, a characteristic that fits the overall goals of the platform. Mobile games were the most likely to be of an arcade type, also potentially due to the affordances and expectation of the mobile platform. Mobile games were not significantly more likely to use attack or defense as a motivation but did account for almost half of the cyber thematic games that did not necessarily cover cybersecurity topics.

As noted previously, these differences associated with the platform on which games can be played have implications as different populations look for games in different places (Duggan, 2015; Juul, 2010). The high number of gamified quizzes and worksheets demonstrate that many game creators are interested in engaging youth with cybersecurity through gameplay but are often using a thin form of games (notably edutainment and gamification) to do so. Games within this genre also tended to be found on platforms that are most accessible across socioeconomic class and technical ability of players. On the other hand, games available through the Steam storefront, which tends to attract players who are more likely to identify with the 'core' gamer identity, presented richer representations of cybersecurity and more meaningful gameplay experiences. Previous work regarding game-based learning has found that there is a balance between giving space to play with concepts within a domain, while also representing those concepts with an appropriate degree of fidelity (Holbert & Wilensky, 2019). Our findings in this review revealed a distinct lack of games that achieved this balance, and the preponderance of those games were not available equitably across platforms. As the cybersecurity field works to broaden participation of underrepresented populations and spread cybersecurity knowledge to the general public, it is important that games are available to all populations and games deeply engaging with cybersecurity content be hosted in places that will reach the broadest set of players.

## *Future Directions for Cybersecurity Game Design*

While this review aims only to present what is currently available, it is clear that there are gaps in the types of games being designed to introduce players to the field of cybersecurity. In particular, the currently available set of cybersecurity games fall short of the promise of games serving as a mechanism to diversify the cybersecurity pipeline and welcome youth from historically underrepresented populations into the world of cybersecurity. For example, this analysis reveals that more work needs to be done to increase the presence of and perception of women and people of color within cybersecurity games. While some games made efforts to represent gender and racially diverse character avatars for players to control, many did not, but instead reflected existing inequities within cybersecurity as a professional field. Best practices for designing games to engage players epistemically with game content suggests that allowing players to choose their representation within these spaces is a powerful tool to further engagement with the domain content (Ryu & Ke, 2018), and that allowing for the creation of avatars that match player identities can greatly increase intrinsic motivation to continue playing a game (Birk et al., 2016).

Games trading simply on the virtue of being a 'game' without engaging deeply with content or game mechanics to attract players run the risk of serving a counter purpose in terms of learning outcomes (Mishra & Foster, 2007), which is worrying for many of the games in this study. Often 'cyber' was used as an aesthetic hook to an unrelated game, and a large portion of the games that did engage with cybersecurity did so in the least meaningful sense as a game - through surface level gamification, or through an edutainment style quiz. There was an encouraging number of games that helped players either work directly with meaningful representations of concepts within cybersecurity (e.g. deep concept engagement), but fewer that also helped players take on meaningful roles as cybersecurity professionals (e.g. epistemic engagement). Given the movement of game-based learning towards these approaches as best practices, we see a great deal of opportunity for future projects to draw from those respective literatures in the design of a cybersecurity game.

Another potential future direction for new cybersecurity videogames is the creation of games that focus on the less-technical aspects of cybersecurity and instead foreground the social aspects of the field. Cybersecurity as a field is multi-faceted and includes a number of socio-technical dimensions (Kessler & Ramsay, 2013). The current landscape of cybersecurity games overwhelming emphasizes the technical aspects of cybersecurity (e.g., passwords and firewalls) and overlook social aspects of the field. Given existing research showing how girls tend to prioritize social interaction and societal good in gameplay (Scott & Zhang, 2014), the inclusion of these types of cybersecurity themes is one potential way to help broaden participation while also shifting perceptions to a more robust and realistic view of the field of cybersecurity.

### *Limitations*

While the systematic analysis of 181 cybersecurity-related games contributes to our understanding of how youth engage with the field in informal settings, the study is not without its shortcomings. For example, the chosen search criteria used to assemble the list of games was based on one particular way of conceptualizing and identifying cybersecurity-related games. This means if a game was trying to introduce players to the field in less explicit ways, or focused solely on one subset of cybersecurity-related skills (e.g. programming) it might not have been captured by the chosen search approach.

A second limitation relates to the self-imposed time limit used for game play. Due to time availability, each story-based game was played for only one hour and each arcade game with repeating levels was played for just thirty minutes. While this gives us an idea of the main ideas of the game, because all the games were not played in full, we cannot be sure that more concepts were not covered later in the game or that new players were not introduced. Additionally, because these games are commercial software, they do not have articles published about their development, content, or intent. Therefore, all information included in this article is based on gameplay rather than information from the game developers.

A third limitation is that we considered games available in English, which may have omitted relevant games developed for other language markets. This choice was motivated both by capacity of the research team, and also as a theoretical choice in our focus on the cybersecurity pipeline in the United States.

A final limitation of this analysis is a result of the rapid rate of change in the game landscape. As the universe of games continues to grow and evolve, by the time the analysis was conducted and the list of cybersecurity games published, it was already starting to fall out of date with respect to the state of the art of the field. While we do not believe this diminishes the value of the work presented, we do acknowledge the fact that there will inevitably be new games that belong as part of this analysis but were released after the initial search.

## Conclusions

This article presents findings from a systematic review of currently-available cybersecurity games aiming to present the current landscape of the games. The findings show how these games have a varied cybersecurity focus and often rely on relatively thin cybersecurity stories and emphasize cybersecurity as an aesthetic or cyber safety. As such, this review shows that few currently available games provide deep content engagement with cybersecurity concepts and fulfill the potential of game-based learning to broaden participation in cybersecurity. This suggests a significant opportunity for game developers and designers interested in issues of education, racial and gender diversity, and cybersecurity. More games need to be made available that offer rich gaming experiences and the opportunity to learn cybersecurity through inquiry. Due to the widespread perception of cybersecurity as a challenging and selective discipline, games can serve as an effective way to introduce cybersecurity to youth. Cybersecurity will continue to be a critical challenge in our increasingly technologically connected world. While the cybersecurity games that are currently available begin to introduce the field to novices, a gap of games deeply engaging individuals who do not already view themselves as potential cybersecurity professionals exists. This suggests the potential for game-based learning to have a significant impact by attracting and introducing cybersecurity broadly to today's youth so as to help grow and diversify the cybersecurity pipeline for years to come.

### Declaration of Conflicting Interests

The authors declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

### Funding

The authors disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: We acknowledge the support of the U.S. Department of Defense. The views and conclusions expressed in this paper are those of the authors and do not necessarily represent those of the Department of Defense or U.S. Government.

## ORCID iD

Merijke Coenraad https://orcid.org/0000-0002-0535-1876

## Note

1. We choose to use the term "minoritized" throughout our work in recognition that the minority status given to people of color is a result of societal constructs lessening the power of members of a group rather than a group only being a small part of the total or less as is implied with "minority."

## References

AMGAMES Inc. (n.d.). *Cyber Defence War* [Mobile game].

Bashir, M., Lambert, A., Wee, J. M. C., & Guo, B. (2015). *An examination of the vocational and psychological characteristics of cybersecurity competition participants*. *Proceedings of the USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE)*.

Birk, M. V., Atkins, C., Bowey, J. T., & Mandryk, R. L. (2016). Fostering intrinsic motivation through avatar identification in digital games. In *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems* (pp. 2982–2995). ACM.

Burley, D., Bishop, M., Kaza, S., Gibson, D. S., Hawthorne, E., & Buck, S. (2017). ACM Joint Task Force on Cybersecurity Education. In *Proceedings of the 2017 ACM SIGCSE Technical Symposium on Computer Science Education – SIGCSE '17* (pp. 683–684). ACM. https://doi.org/10.1145/3017680.3017811

Calleja, G. (2011). *In-game: From immersion to incorporation*. The MIT Press.

Carnegie Mellon University. (2019). *Catch the Software Bugs* [Flash game]. http://www.carnegiecyberacademy.com/funStuff/catchBugs/summerReadingBugs.html

Center for Cyber Safety and Education. (2017). *2017 global information security workforce study*. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

Clark, D., Tanner-Smith, E., & Killingsworth, S. (2016). Digital Games, design, and learning: A systematic review and meta-analysis. *Review of Educational Research*, *86*(1), 79–122. https://doi.org/10.3102/0034654315582065

Clinkenbeard, I. (2018). *Obio* [Mobile game].

Connolly, T. M., Boyle, E. A., MacArthur, E., Hainey, T., & Boyle, J. M. (2012). A systematic literature review of empirical evidence on computer games and serious games. *Computers & Education*, *59*(2), 661–686. https://doi.org/10.1016/j.compedu.2012.03.004

Dark, M. (2002). *Defining a curriculum framework in information assurance and security* (Cerias Technical Report). CERIAS, Purdue University.

Digital Eel. (2011). *Data Jammers: FastForward* [PC game].

Duggan, M. (2015). *Gaming and gamers* (Research Report). Pew Research Center. https://www.pewinternet.org/2015/12/15/gaming-and-gamers/

Federal Bureau of Investigation. (n.d.). *Safe Online Surfing* [Online game]. U.S. Department of Justice. https://sos.fbi.gov/en/

Florida State University. (2018). *Cyber Bowl* [Online game]. https://cyberbowl.its.fsu.edu/game/

Gee, J. P. (2004). *Situated language and learning: A critique of traditional schooling*. Routledge.

Gee, J. P. (2005). Good video games and good learning. *Phi Kappa Phi Forum*, *85*(2), 33–38.

Gee, J. P. (2007). *What video games have to teach us about learning and literacy*. Palgrave Macmillan.

Gestwicki, P., & Stumbaugh, K. (2015). Observations and opportunities in cybersecurity education game design. In *2015 Computer Games: AI, Animation, Mobile, Multimedia,*

*Educational and Serious Games (CGAMES)* (pp. 131–137). https://doi.org/10.1109/CGames.2015.7272970

Google. (n.d.). *Interland: Be Internet Awesome* [Online game]. https://beinternetawesome.withgoogle.com/en_us/interland/

Holbert, N., & Wilensky, U. (2019). Designing educational video games to be objects-to-think-with. *Journal of the Learning Sciences*, *28*, 37–72. https://doi.org/10.1080/10508406.2018.1487302

i273 LLC. (2016). *Hack NET* [Mobile game].

Iacovides, I., McAndrew, P., Scanlon, E., & Aczel, J. (2014). The gaming involvement and informal learning framework. *Simulation & Gaming*, *45*(4–5), 611–626. https://doi.org/10.1177/1046878114554191

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. (2018). Evaluation of Game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150. https://doi.org/10.11591/edulearn.v12i1.7736

Juul, J. (2010). *A casual revolution: Reinventing video games and their players*. The MIT Press.

Katsaliaki, K., & Mustafee, N. (2015). Edutainment for sustainable development: A survey of games in the field. *Simulation & Gaming*, *46*(6), 647–672. https://doi.org/10.1177/1046878114552166

Kessler, G. C., & Ramsay, J. (2013). Paradigms for cybersecurity education in a homeland security program. *Journal of Homeland Security Education*, *2*, 35–44.

Ketelhut, D. J. (2007). The impact of student self-efficacy on scientific inquiry skills: An exploratory investigation in River City, a Multi-user Virtual Environment. *Journal of Science Education and Technology*, *16*(1), 99–111. https://doi.org/10.1007/s10956-006-9038-y

Konijn, E., & Bijvank, M. (2009). Doors to another me: Identity construction through digital game play. In U. Ritterfeld, M. J. Cody, & P. Vorderer (Eds.), *Serious games: Mechanisms and effects* (pp. 201–225). Routledge.

Ladabouche, T., & LaFountain, S. (2016). GenCyber: Inspiring the next generation of cyber stars. *IEEE Security & Privacy*, *14*(5), 84–86.

Landis, J. R., & Koch, G. (1977). The measurement of observer agreement for categorical data. *Biometrics*, *33*(1), 159–174.

Liberati, A., Altman, D. G., Tetzlaff, J., Mulrow, C., Gøtzsche, P. C., Ioannidis, J. P. A., . . . Moher, D. (2009). The PRISMA statement for reporting systematic reviews and meta-analyses of studies that evaluate health care interventions: Explanation and elaboration. *PLOS Medicine*, *6*(7), Article e1000100. https://doi.org/10.1371/journal.pmed.1000100

Life Education Australia. (2018). *bCyberwise Monster Family* [Mobile game]. https://www.lifeeducation.org.au/children/bcyberwise-app

Lopes, M. C., Fialho, F. A. P., Cunha, C. J. C. A., & Niveiros, S. I. (2013). Business games for leadership development: A systematic review. *Simulation & Gaming*, *44*(4), 523–543. https://doi.org/10.1177/1046878112471509

Mishra, P., & Foster, A. (2007). The claims of games: A comprehensive review and directions for future research. In R. Carlsen, K. McFerrin, J. Prince, R. Weber, & A. D. Willis (Eds.), *Proceedings of SITE 2007* (pp. 2227–2232). AACE.

Osmotic Studios. (2016). *Orwell: Keeping an Eye On You* [PC game]. Fellow Traveller.

Pusey, P., Gondree, M., & Peterson, Z. (2016). The outcomes of cybersecurity competitions and implications for underrepresented populations. *IEEE Security & Privacy*, *14*(6), 90–95.

Rebelephant. (2017). *Mainlining* [Steam PC game]. Merge Games.

Reckien, D., & Eisenack, K. (2013). Climate change gaming on board and screen: A review. *Simulation & Gaming*, *44*(2–3), 253–271. https://doi.org/10.1177/1046878113480867

Reed, J., & Acosta-Rubio, J. (2017). *Innovation through inclusion: The multicultural cybersecurity workforce—An (ISC)² 2017 Global Information Security Workforce Study*. https://iamcybersafe.org/wp-content/uploads/2018/04/Multicultural-Diversity-Report-2018.pdf

Ricci, M., & Gulick, J. (2017). Cybersecurity games: Building tomorrow's workforce. *Journal of Law & Cyber Warfare*, *5*(2), 183–224.

Ryu, J., & Ke, F. (2018). Increasing persona effects: Does it matter the voice and appearance of animated pedagogical agent. *Educational Technology International*, *19*(1), 61–91.

Saldaña, J. (2015). *The coding manual for qualitative researchers* (3rd ed.). SAGE.

Scott, K., & Zhang, X. (2014). Designing a culturally responsive computing curriculum for girls. *International Journal of Gender, Science and Technology*, *6*(2), 264–276.

Shumba, R., Hall, L., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., & Bace, R. (2013). *Cybersecurity, women and minorities: Findings and recommendations from a preliminary investigation*. ACM Press. https://doi.org/10.1145/2543882.2543883

Sitzmann, T. (2011). A meta-analytic examination of the instructional effectiveness of computer-based simulation games. *Personnel Psychology*, *64*, 489–528. https://doi.org/10.1111/j.1744-6570.2011.01190.x

Skunkape Interactive. (2015). *ROOT* [PC game]. Digital Tribe.

Squire, K. (2006). From content to context: Videogames as designed experience. *Educational Researcher*, *35*(8), 19–29. https://doi.org/10.3102/0013189X035008019

Squire, K., & Jenkins, H. (2011). *Video games and learning: Teaching and participatory culture in the digital age*. Teachers College Press.

Svabensky, V., & Vykopal, J. (2018). Gathering insights from teenagers' hacking experience with authentic cybersecurity tools. In *2018 IEEE Frontiers in Education Conference (FIE)* (pp. 1–4). https://doi.org/10.1109/FIE.2018.8658840

Svabensky, V., Vykopal, J., & Celeda, P. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In *The 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*. ACM. https://doi.org/10.1145/3328778.3366816

Symantec Corp. (2018). *Internet security threat report*. https://doi.org/10.1007/s10207-014-0262-9

Texas A&M Division of Information Technology. (2017). *Keeping Tradition Secure* [Online game]. https://security.tamu.edu/Cyber_Security_Games.php

Thirteen Productions LLC. (2019). *PBS Kids: CyberChase*. https://pbskids.org/cyberchase/

Tobey, D. H., Pusey, P., & Burley, D. L. (2014). Engaging learners in cybersecurity careers: Lessons from the launch of the national cyber league. *ACM Inroads*, *5*(1), 53–56. https://doi.org/10.1145/2568195.2568213

Tulip Project. (n.d.). *Firewall Administration* [Online game]. University of Edinburgh School of Informatics. https://sites.google.com/site/firewallgameinf/home

Turner, L. (2009). Gender diversity and innovative performance. *International Journal of Innovation and Sustainable Development*, *4*(2–3), 123–134. https://doi.org/10.1504/IJISD.2009.028067

Vogel, J. J., Vogel, D. S., Cannon-Bowers, J., Bowers, C. A., Muse, K., & Wright, M. (2006). Computer gaming and interactive simulations for learning: A meta-analysis. *Journal of Educational Computing Research*, *34*, 229–243.

Wee, J. M. C., Bashir, M., & Memon, N. (2016). *Self-efficacy in cybersecurity tasks and its relationship with cybersecurity competition and work-related outcomes* [Paper presentation]. USENIX Security Symposium, Austin, TX, 9 August 2016.

WGBH Educational Foundation. (2014). *Cyber Lab* [Online game]. PBS Online. https://www.pbs.org/wgbh/nova/labs/lab/cyber/research#/newuser

Wouters, P., van Nimwegen, C., van Oostendorp, H., & van der Spek, E. D. (2013). A meta-analysis of the cognitive and motivational effects of serious games. *Journal of Educational Psychology*, *105*, 249–265. https://doi.org/10.1037/a0031311

Yang, Y., & Konrad, A. M. (2011). Diversity and organizational innovation: The role of employee involvement. *Journal of Organizational Behavior*, *32*, 1062–1083.

## Author Biographies

**Merijke Coenraad** is a PhD Candidate in the Department of Teaching & Learning, Policy & Leadership in the College of Education at the University of Maryland. Her research focuses on the intersections of educational technology and equity including the creation of materials, platforms, and experiences in partnership with teachers and youth through participatory design methods.

Contact: mcoenraa@umd.edu

**Anthony Pellicone** is a post-doctoral researcher at the University of Maryland, College Park. His research uses a mixture of methods to study how people learn, socialize, and play in games. Anthony's work has focused on topics such as online game cultures, social roles in online gameplay, and the design of games to promote interest and identity formation.

Contact: apellico@umd.edu

**Diane Jass Ketelhut** is professor of STEM education. Her research focuses on improving self-efficacy (in computational thinking and science) and learning through scientific inquiry experiences within immersive environments. Her research stems across all grades and ages, student and teacher. Diane holds a doctorate in Learning & Teaching from the Harvard Graduate School of Education, and previously served as a classroom teacher in multiple states for 12 years.

Contact: djk@umd.edu

**Michel Cukier** is a professor of reliability engineering with a joint appointment in the Department of Mechanical Engineering at the University of Maryland, College Park. He is also the director for the Advanced Cybersecurity Experience for Students (ACES). His research covers dependability and security issues. Dr. Cukier has published more than 70 papers in journals and refereed conference proceedings in those areas.

Contact: mcukier@umd.edu

**Jan Plane** is a principal lecturer in the Department of Computer Science and the Associate Director for the Advanced Cybersecurity Experience for Students (ACES). She is also the Director of the Iribe Initiative for Inclusion and Diversity in Computing (I4C) and the Maryland Center for Women in Computing (MCWIC) where she supports diversity of the field through education for all age groups.

Contact: jplane@umd.edu

**David Weintrop** is an assistant professor in the Department of Teaching & Learning, Policy & Leadership in the College of Education with a joint appointment in the College of Information Studies at the University of Maryland. His research focuses on the design, implementation, and evaluation of accessible, engaging, and equitable computational learning experiences. His work lies at the intersection of design, computational thinking education, and the learning sciences.

Contact: weintrop@umd.edu