Designing a Game to Promote Equity in Cybersecurity

Anthony Pellicone, Diane Jass Ketelhut, Ekta Shokeen, David Weintrop, Michel Cukier and Jandelyn Dawn Plane
University of Maryland, College Park, USA
apellico@umd.edu
djk@umd.edu
eshokeen@umd.edu
weintrop@umd.edu
jplane@umd.edu

Abstract: Cybersecurity faces a persistent problem with attracting and retaining diverse workers. Most exposure to cybersecurity as a discipline tends to come through formal experiences in higher education, often requiring extensive prior experience with computer science content. Therefore, informal learning environments that can serve to both introduce youth to concepts found within cybersecurity, as well as aiding them in building identities as the type of person who can 'do' cybersecurity, may be able to advance the goal of diversifying the field. Game-based learning is an effective approach for attracting new learners to specific domains of knowledge in informal contexts. Players who might not otherwise think of themselves as being capable participants within a field can use the structures and supports commonly found in well-designed digital games to build a personal identity as a novice practitioner of that domain. Previous work has found that while cybersecurity is represented in some commercial games, the depiction tends to be either superficial, or when there is a deeper engagement with content, tends to represent a stereotypical personage of a cybersecurity professional. In this paper, we present a digital game, called *HEX of The Turtle Islands* (*HEX*), designed to introduce players from historically underrepresented populations to the domain of cybersecurity. *HEX* leverages several gameplay elements to immerse players in a learning experience centered on cybersecurity: rich, multi-layered narratives; building player self-efficacy and identity within the domain of cybersecurity through challenges rooted in concepts that are authentic to the field; and making the game broadly accessible in terms of technology and design. In introducing HEX, we discuss how the design of the game can broaden participation in cybersecurity and conveys authentic cybersecurity concepts to players. Drawing from 2 years of playtesting data with a diverse group of youth play testers, we discuss both challenges and opportunities for introducing underrepresented youth to cybersecurity through play.

Keywords: game-based learning, cybersecurity, game design, self-efficacy, equity

1. Introduction

Cybersecurity is an interdisciplinary practice, which bridges people, technology, and networks that comprise our modern information society (Bambauer et al., 2021; Burley et al., 2017). However, cybersecurity faces a persistent problem with attracting and retaining diverse workers (Reed & Acosta-Rubio, 2017) - namely women, people of color, indigenous populations, workers with disabilities, and other minoritized populations. Most exposure to cybersecurity as a discipline tends to come through formal experiences in higher education, which often require significant prior computer science coursework, where these populations have been historically excluded (Burrell & Nobles, 2018; Dark, 2002). Other technical disciplines also have a 'bottleneck' problem, where the formal pipeline through education is gates by experiences that are alienating to minoritized students and women (Shumba et al., 2013). The bottleneck issue in cybersecurity is compounded by the way that it is typically taught as a capstone in computer science, meaning learners are only introduced to it at the tail end of their academic careers (Reed & Acosta-Rubio, 2017). While there are several informal initiatives to broaden cybersecurity participation in primary and secondary education (e.g. Gen-Cyber), these are often restricted to in-person events that are limited in scope (Ricci & Gulick, 2017; Tobey et al., 2014). These initiatives, which are often structured as game-like experiences, are shown to be effective at increasing interest in cybersecurity, but are necessarily limited by time, space, and access (Wee et al., 2016). Therefore, informal learning environments that can serve to both introduce youth to concepts found within cybersecurity, as well as aid them in building identities as people who can 'do' cybersecurity are appealing to the larger goal of diversifying the field (Jin et al., 2018).

Game-based learning has been shown to be effective at introducing learners to self-efficacious experiences (Connolly, et al., 2012; Gee, 2009; Ketelhut, 2007), and allow players to engage with content area skills and knowledge (Clark et al., 2016; Holbert & Wilensky, 2017). Relatedly, games are currently widely enjoyed by youth of all backgrounds and demographics (Duggan, 2015; Juul, 2010). Therefore, there is great potential in creating cybersecurity gaming experiences that can serve as an introduction to the field, thus diversifying the profession

as a whole. In this paper, we report on our efforts to design such a game for the field of cybersecurity, titled *HEX of the Turtle Islands* (*HEX*), and pursue the following overarching research question: *How can the affordances of digital games and play be used to broaden participation in cybersecurity?*

2. Promoting Equity in Cybersecurity and Game Design Implications

As with other technical disciplines, cybersecurity professionals are usually trained through formalized coursework in higher education. Like other career paths, the trajectory of a cybersecurity professional is unique to the field itself, influenced by both formal and informal experiences (Cannady, Greenwald & Harris, 2014) as well as the background and identity of the learner (Calabrese Barton et al., 2012). Due to the interdisciplinarity nature of cybersecurity and its academic positioning as a subfield of computer science, it is often not taught formally until the upper levels of computer science higher education (Dark, 2002). As a result, only students who have completed years of computer science coursework have the opportunity to learn about cybersecurity courses. This has direct implications for the diversity of the field, as computer science has long struggled to recruit and retain a student body the reflects the racial, socio-economic, and gender demographics of the larger population (Zweben et al., 2020). Game-based learning presents a way to address this issue by introducing learners to fields where they are underrepresented, allowing them to build self-efficacy and identities within those domains (Ketelhut, 2006), experience domain-authentic representations of concepts (Holbert & Wilensky, 2017), and to build identities as practitioners within those domains (Gee, 2006; Squire, 2006). Previous work has found that games often use cybersecurity superficially as a visual or narrative aesthetic, but infrequently convey authentic concepts from the domain (Coenraad et al, 2020; Gestwicki & Stumbaugh, 2015). In terms of the goal of diversifying the cybersecurity workforce, Coenraad et al. (ibid) also found that in games that have more conceptually accurate representations of cybersecurity, there is also a lack of diversity in representation of the player's avatar and in non-player characters. Thus, for games to serve as a mechanism to broaden participation in cybersecurity, they need to more authentically engage players with concepts in cybersecurity and do so in a way that promotes equity in the cybersecurity workforce.

Given the goal of this work, we pursued the design of HEX with three primary design considerations: (1) Multiple Intertwined Narratives, (2) Authentic Representations of Cybersecurity and Computational Thinking Concepts, and (3) Tying Narrative and Puzzle Elements Together Through Exploration as a Game Mechanic. Since our goal is to appeal to populations who are not well represented in cybersecurity (thus expanding equity), **multiple Intertwined Narratives** can serve as 'hooks' to draw a broader array of players into the game. Narrative is an essential element of game-based learning in terms of driving player immersion and engagement (Jemmali et al., 2018; Naul & Liu, 2020), however narratives that are either alienating or distracting can have negative impacts on learning outcomes (Dickey, 2011). Game design literature indicates that many of the youth in our target demographic prefer game narratives that focus on the idea of helping others (Graner-Ray, 2004). Therefore, *HEX*'s narrative includes three intertwined narratives: a central story related to helping and rescuing characters who are close to the player, a related narrative about maintaining the ecological health of a unique island ecosystem, and an overarching narrative relating to a growing cybersecurity threat from a shadowy corporation. Given that cybersecurity historically attracts individuals who are already interested in computer science (Center for Cyber Safety and Education, 2017), we wanted to create numerous opportunities for players to both see themselves as capable of tackling cybersecurity challenges, and to use the embodied nature of gameplay (Squire, 2006) to connect their actions in-game with their personal identities. Thus, it is important the game have **Authentic Representations of Cybersecurity and Computational Thinking Concepts.** This has informed the design decisions of embedding cybersecurity activities into the two narrative themes to provide motivation to pursue those themes, to provide significant scaffolds for the cybersecurity activities, and to provide vicarious experiences through NPC 'friends.' The game supports identity formation through the implementation of a dynamic avatar system to allow the player to create a projective identity within the game world (Birk et al., 2016; Gee, 2007). Finally, the game seeks to **tye Narrative and Puzzle Elements Together Through Exploration as a Game Mechanic.** Given the interdisciplinary nature of cybersecurity (Bambauer et al., 2021; Burley et al., 2017), we have made a mechanical decision to incorporate both narrative and conceptual elements into a rich, explorable world, which ties together both the social and technical aspects of cybersecurity.

2.1 Introducing HEX of the Turtle Islands

HEX is a game that combines rich narrative, puzzles and challenges rooted in cybersecurity concepts, and gameplay focused on exploration. In *HEX,* players take on the role of a youth participating in a summer work study program investigating recent changes in the ecology around a remote island chain called *The Turtle Islands*. During their trip, their boat is boarded by pirates, and the crew is kidnapped, requiring the player to investigate

a larger conspiracy involving the shadowy corporation known as HEX. The players encounter cybersecurity challenges that they must solve to find out what is happening, rescue the crew, and help save the world.

The game takes the form of a 2-dimensional isometric adventure game, with a design and perspective similar to the *Legend of Zelda: A Link to the Past* (Nintendo, 1991). The current build of the game focuses on one island of the game and provides a tutorial for basic game mechanics, sets up the three primary narrative strands, and introduces players to puzzles that focus on ciphers (Fig 1.a), computational logic (Fig 1.b), pathing (Fig 1.c), modular arithmetic (Fig 1.d), and non-conceptual puzzles such as box pushing (Fig 1.e).

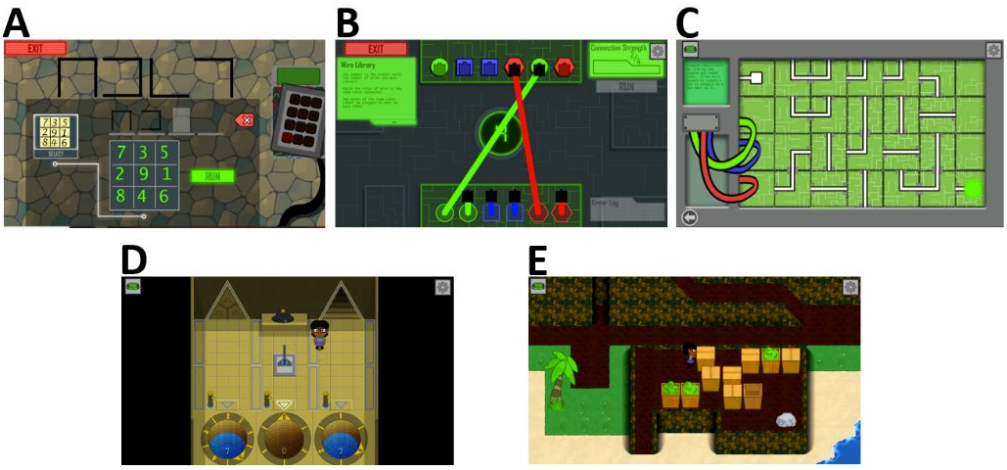

Figure 1: The five primary puzzles in the current build of the game. Label A is a simple cipher that matches numbers on a keypad to shapes on a 3 by 3 grid, B is a wire matching puzzle that is based on computational logic, C is a pathing puzzle where players must connect two sides of a circuit, D is a modular arithmetic puzzle where players use concepts from modular arithmetic to balance water between three wells, and E is an example of an environmental obstacle (in this case pushing boxes to reach an objective)

3. Playtesting Methodology and Data Analysis

HEX has been play tested by 31 participants between the ages of 10 and 16 through in-person and online playtesting sessions. Our target age range is 10 to 13, and data from this age range was prioritized in our preliminary analysis, however due to our recruitment and data collection taking place in public libraries we increased the age range to 16 to allow for older siblings who may be responsible for their younger siblings' aftercare to participate as well. Participation was incentivized with a $15 Amazon gift certificate, and both parental consent and child assent was collected for each participant. The demographics of our sample are reported in Table 1 below. For our findings we include in-text notation to describe participants (e.g. Female, 12, African American), along with a pseudonym assigned to match the participant's stated gender. For each session we collected the participant's play data, which was recorded through a novel method of data collection where players were asked to frame their responses to the game as live-streaming (Pellicone et al., 2022). Play sessions averaged around 45 minutes and included both player commentary and recorded gameplay. At the conclusion of the session, we asked a series of interview questions about the gameplay experience.

Table 1: A table of the reported demographics of our sample

	Male	**Female**	**White**	**Black or African American**	**Asian or Pacific Islander**	**Hispanic, Latino, or Spanish Origin**	**Not Reported**
Number of Players Reported	18	13	10	9	5	3	4

We are following Fullterton's (2014) approach to playtesting, which calls for consistent, iterative, play-centric testing across the development cycle of a game. Thus, the data that we present in this paper comes from multiple evolving versions of the game, as well as targeted playtesting data for specific puzzles. The methods employed across these iterative sessions included cooperative inquiry, think aloud protocols, and traditional playtesting. Data was analysed using an open, interpretive grounded theory method (Charmaz, 2014). Authors 1 and 3

engaged in consensus coding (Charmaz, 2014; Stemler, 2019) through consistent debriefing, memoing, and coding across several rounds of playtesting. Consensus was reached through the two coders through an iterative process of collecting data, reviewing it line by line, and discussing emerging themes throughout the analytic process (Cascio, Lee & Vaudrin, 2019; Stemler, 2019). Through this iterative method of analysis, we reached theoretical saturation for this stage of the game design process (Star, 2007). The central themes that emerged through the analysis serve as the headings for our findings section below.

4. Preliminary Findings

Our findings emerged around three themes that corresponded to the design of our game: (1) how players responded to the **narrative** of the game; (2) how players responded to **the cybersecurity and computational thinking concepts** contained in our puzzles; and (3) how they experienced these elements combined through gameplay that focuses on **exploring an interactive world**. The bolded themes above evolved from a higher level codebook that focused on:

- multiple 'hooks' present in the game, meaning designed elements meant to attract a broad range of players – these were the primary kidnapping plotline, the ecological storyline, cybersecurity and computational thinking, and helping characters and NPCs to solve problems;
- puzzle solving behaviour from players, meaning player verbal and non-verbal responses to the challenges in the game (see Figure 1), as well as player responses in interviews to questions about strategies and conceptions of the in-game puzzles;
- player engagement with non-puzzle mechanics which serve to tie the game experience together, for example the interactive narrative elements, and the game-world and level design;

From across these broad initial codes, we narrowed our codebook into the subject headings which serve as our findings, and are presented below.

4.1 The Importance of Multiple Narrative Hooks

Overall, players reacted positively to the presence of multiple narrative hooks. An example of this comes from Kevin (Male, 14, White), who responded to an interactive storytelling element early in the game, which takes the form of a cork-board that tracks the actions of the mysterious HEX corporation, saying, "*HEX is behind her disappearance? What the heck is HEX?*" Later in his interview while sharing about his views about the narrative, he said, *"I have a feeling it'll go into more about the corporation thing, the HEXCorp, but it could also easily go into like what crashed the ship … I'm probably going to have to break into some kind of HEX Corp headquarters or something like that.*" This matches to our larger goal to use HEX-related elements to bring more cybersecurity elements into the narrative by having players follow a narrative path that asks them to both attack and secure networked systems in pursuit of rescuing the kidnapped crew from HEX. Similarly, the ecological storyline serves as a hook for other players. One example comes from Darren (Male, 12, African American) who responded to a small environmental puzzle where players must find sea turtles aboard the starting boat area, saying, "*In the introduction, like before the game, it explained that you're on this boat trip with these other people – other students and professionals – and you can interact with the things, and even though you don't need to learn what each person does it is cool to know that. Then you have to help find the turtles, and it's cool because they're all around the place.*" In addition to the thematic elements of the narrative, we have also been using a guiding design consideration to have the player help other NPC and also save the ecosystem of the island. Casandra (Female, 13, unknown) responded extremely positively to the game, and when asked about the purpose of the game says that it's about "*be[ing] friends with people, and helping them out.*" Steven (Male, 13, African American) said that an enjoyable aspect of the game was that "*even though some bad things may happen, we can still fix it."* Having multiple threads appealing to different aesthetic and narrative approaches allows us to 'hook' players with differing interests and guide them towards cybersecurity aspects of the game.

4.2 Balancing Scaffolding and Discovery

Across the five puzzles currently in the game, we have gathered data revealing how to convey the complex ideas that underly cybersecurity in a way that both supports novice learning while also providing the thrill of discovery. An example of this was identified in early iterations of the wire puzzle, where we observed players not understanding the logical rules that underpin the puzzle's gameplay, which were initially contained entirely in a text-box on the side of the screen (see Fig 2.b). This was clear in Alex's (Male, 12, African American) playtesting data when he read the entire set of instructions, stumbling when he got to the final rule, "*Same color wires cannot be in neighbouring ports.*" After reading this, he sighed, and said, *"Oooook… I kinda' don't understand.*"

As he continued, he became more visibly frustrated. While the previous puzzles had offered a layered series of clues situated within the narrative (e.g., the players find a cipher and connect this to a visual hint of the key on the wall, along with hints from the NPC friend characters), the wire puzzle instead relied entirely upon the player's ability to read and interpret the written rules. After over 4 minutes of struggling with this puzzle (gameplay up to this point had taken approximately 10 minutes), Alex begins to understand the rule about wires not being able to be placed in matching ports. He ultimately succeeded in figuring out the correct configuration, and said, "*Ok then. It doesn't want me to put those wires together. [sarcastically] What beautiful logic*." Although Alex enjoyed the game overall, this interaction pointed us towards an important design change, and led us to embed the wire puzzle rules into collectible items in the game-world, along with modifications to the language of the hints. Through subsequent testing we found that players became stuck on this puzzle less often, indicating the success of this approach.

4.3 The Tricky Balance of Exploration

Our participants have had a wide array of prior gaming experience resulting in varying success in our use of exploration as a game mechanic. A frequent design tension has been finding the right balance between allowing players to explore and directing them productively through levels. An example can be seen with Nicolas (Male, 12, Hispanic, Latino, or Spanish Origin), who enjoyed the first relatively linear part of the game, but, as gameplay becomes more open, Nicolas became frustrated and not sure what to do next, saying "*Oh my god… what am I supposed to do!*" Nicolas eventually asked for facilitator help in navigating this portion of the level. In his interview, Nicolas expressed engagement with the puzzles, but said that exploring the level was the most frustrating aspect of his experience. Nicolas also mentioned that he plays games infrequently, and most commonly multi-player sports games. More experienced players found this aspect of exploration to be enjoyable, like John (Male, 14, White), who upon seeing the more open beach level remarked, "*This way does not seem like the right way. Where in the world do I need to go? Well, I guess it's less straightforward now. So that's nice*." Consistently across our data, players with less prior gaming experience had difficulty with exploration, however as discussed below, exploration is still a priority for the design of our game.

5. Discussion, Limitations, Next Steps, and Conclusions

5.1 Discussion

Through our iterative design and testing process, we identify three design conclusions.

1. **Multiple narrative hooks are a productive way to introduce players to a complex domain like cybersecurity.** Considering our demographic and the desire to provide multiple pathways into cybersecurity, this is a very positive finding, and helps to inform our approach going forward. We present this as a design consideration for other designers seeking to broaden participation in any field.
2. **By situating puzzles in rich, explorable worlds, designers can ease players into a domain that is necessarily complex and multi-layered.** We can see this clearly in Alex's example, and as this was an early finding through our playtesting process, it has also been a valuable guiding design consideration in our process.

Given the above, this also requires us to (3) create a gameplay experience that incorporates exploration as a core gameplay mechanic. While some players reacted positively to this design, other players respond negatively to exploration. This is a tricky problem to solve, and one that we are still actively working on and see as a productive avenue for further research.

5.2 Limitations and Conclusions

Our goal for this work is to introduce cybersecurity to youth through narrative and puzzle mechanics. As we are still in the design phase, we cannot yet make claims about affective or learning outcomes but we do see players being drawn gradually to cybersecurity through the game. This also represents small-scale qualitative playtesting, which is reasonable given where we are in the design process. It also limits the generalizability of the claims reported here. Moving forward, we plan to roll the game out to a wider audience and will evaluate player behaviors at scale while also expanding the game narrative and further developing and deploying the game design principles outlined in this work. A second ongoing strand of research is to understand player reactions across demographics. Although this showed itself to some degree in our current data analysis, this is a dimension of our data we wish to understand more completely as our analytic work progresses.

As with any game development process, our game has limitations due to the structure of our team. We recognize that cooperative inquiry (e.g. Druin, 1999) could be productively used to understand player reactions to cybersecurity content, and we did use cooperative inquiry for initial ideation during the game development process. Further usage of cooperative inquiry to design challenges, narratives, and mechanics is work that we would like to pursue in the future, but for the work presented above we have limited our testing efforts to think-aloud protocols and traditional playtesting methods.

Altogether we find that game-based learning represents a rich educational context to introduce underrepresented learners to the domain of cybersecurity. We have described several affordances of game-based learning that we have leveraged in the design of *HEX*, and we offer these preliminary findings to other designers seeking to create similar games.

Acknowledgements

We acknowledge the funding support of the 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. Most of all, we like to thank students who participated in this study for sharing their experiences with us.

References

Bambauer, D. E., Hurwitz, J. (Gus), Thaw, D., & Tschider, C. A. (2021). *Cybersecurity: an interdisciplinary problem*. West Academic Publishing.

Birk, M. V., Atkins, C., Bowey, J. T., & Mandryk, R. L. (2016). "Fostering Intrinsic Motivation through Avatar Identification in Digital Games", *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*, 2982–2995. https://doi.org/10.1145/2858036.2858062

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

Burrell, D., & Nobles, C. (2018). "Recommendations to develop and hire more highly qualified women and minorities cybersecurity professionals", *Proceedings of the 2018 ICCWS*. International Conference on Cyber Warfare and Security, Albany, NY.

Calabrese Barton, A., Kang, H., Tan, E., O'Neill, T. B., Bautista-Guerra, J., & Brecklin, C. (2012). "Crafting a future in science: Tracing middle school girls' identity work over time and space", *American Educational Research Journal*, *50*(1), 37–75. https://doi.org/10.3102/0002831212458142

Center for Cyber Safety and Education. (2017). *2017 global information security workforce study*. https://iamcybersafe.org/wp-content/uploads/2017/06/Europe Cascio, M. A., Lee, E., Vaudrin, N., & Freedman, D. A. (2019). A Team-based Approach to Open Coding: Considerations for Creating Intercoder Consensus. *Field Methods*, *31*(2), 116–130. https://doi.org/10.1177/1525822X19838237

-GISWS-Report.pdf

Charmaz, K. (2014). *Constructing grounded theory* (2nd edition). Sage.

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). "Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games", *Simulation & Gaming*, *51*(5), 586–611. https://doi.org/10.1177/1046878120933312

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.

Dickey, M. D. (2011). "Murder on Grimm Isle: The impact of game narrative design in an educational game-based learning environment", *British Journal of Educational Technology*, *42*(3), 456–469. https://doi.org/10.1111/j.1467-8535.2009.01032.x

Fullerton, T. (2014). *Game design workshop: a Playcentric approach to creating innovative games*.

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

Gee, J. (2009). "Deep learning properties of good digital games: How far can they go?", In U. Ritterfeld, M. J. Cody, & P. Vorderer (Eds.), *Serious games: mechanisms and effects* (pp. 67–82). Routledge.

Gestwicki, P., & Stumbaugh, K. (2015). "Observations and opportunities in cybersecurity education game design", *2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES)*, 131–137. https://doi.org/10.1109/CGames.2015.7272970

Jemmali, C., Bunian, S., Mambretti, A., & El-Nasr, M. S. (2018). "Educational game design: an empirical study of the effects of narrative", *Proceedings of the 13th International Conference on the Foundations of Digital Games*, 1–10. https://doi.org/10.1145/3235765.3235783

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

Naul, E., & Liu, M. (2020). "Why Story Matters: A Review of Narrative in Serious Games", *Journal of Educational Computing Research*, *58*(3), 687–707. https://doi.org/10.1177/0735633119859904

Pellicone, A., Weintrop, D., Ketelhut, D. J., Shokeen, E., Cukier, M., Plane, J. D., & Rahimian, F. (2022). Playing Aloud: Leveraging Game Commentary Culture for Playtesting. *International Journal of Gaming and Computer-Mediated Simulations*, *14*(1), 1–16. https://doi.org/10.4018/IJGCMS.296705

Reed, J., & Acosta-Rubio, J. (2017). *Innovation through inclusion: The multicultural cybersecurity workforce* (pp. 1–9). https://www.isc2.org/-/media/Files/Research/Innovation-Through-Inclusion-Report.ashx

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

Ray, S.G., 2003. *Gender Inclusive Game Design: Expanding the Market (Advances in Computer Graphics and Game Development Series)*. Charles River Media, Inc..

Squire, K. (2006). "From Content to Context: Videogames as Designed Experience", *Educational Researcher*, *35*(8), 19–29. https://doi.org/10.3102/0013189X035008019

Star, S. L. (2007). "Living ground theory", In K. Charmaz & A. Bryant (Eds.), *The Sage Handbook of Grounded Theory* (pp. 75–94). SAGE.

Stemler, S. (2019). "A Comparison of Consensus, Consistency, and Measurement Approaches to Estimating Interrater Reliability", *Practical Assessment, Research, and Evaluation*, *9*(1). https://doi.org/https://doi.org/10.7275/96jp-xz07

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

Zweben, S. H., Tims, J. L., Tucker, C., & Timanovsky, Y. (2021). ACM-NDC study 2020--2021: ninth annual study of non-doctoral-granting departments in computing. *ACM Inroads*, *12*(4), 30–44. https://doi.org/10.1145/3485245