Observations and Opportunities in Cybersecurity Education Game Design

Paul Gestwicki and Kaleb Stumbaugh
Computer Science Department
Ball State University
Muncie, IN 47306
Email: pvgestwicki@bsu.edu

***Abstract*—We identify three challenges in cybersecurity education that could be addressed through game-based learning: conveying cybersecurity fundamentals, assessment of understanding, and recruitment and retention of professionals. By combining established epistemologies for cybersecurity with documented best practices for educational game design, we are able to define four research questions about the state of cybersecurity education games. Our attention is focused on games for ages 12–18 rather than adult learners or professional development. We analyze 21 games through the lens of our four research questions, including games that are explicitly designed to teach cybersecurity concepts as well as commercial titles with cybersecurity themes; in the absence of empirical evidence of these games' efficacy, our analysis frames these games within educational game design theory. This analysis produces a three-tier taxonomy of games: those whose gameplay is not associated with cybersecurity education content (Type 1); those that integrate multiple-choice decisions only (Type 2); and those that integrate cybersecurity objectives into authentic gameplay activity (Type 3). This analysis reveals opportunities for new endeavors to incorporate multiple perspectives and to scaffold learners progression from the simple games to the more complex simulations.**

Keywords: cybersecurity education, educational games, game analysis, game design

I. Introduction

The 2014 Cybersecurity Education Workshop Final Report [1] highlights several areas for growth and development in cybersecurity education. We were inspired by the *Concepts and Conceptual Understanding*, *Assessment*, and *Recruitment and Retention* recommendations in particular. The first deals with conveying fundamentals of cybersecurity, not just to information technology professionals but to anyone whose work intersects modern technology—that is, practically everyone in the developed world. A challenge posed by the report is to deal with the fundamental epistemological question: what is cybersecurity? The second deals with the problem of assessing efficacy of educational interventions. That is, if we design a cybersecurity education intervention, how do we know that the participant has learned something? Of particular interest is transfer: it is not sufficient for the learning to be embedded only in the intervention when the goal is to affect behaviors outside of it. The third recommendation inspiring this work deals with the pipeline problem. Maintaining our current technology and information infrastructure requires a critical number of well-prepared knowledge workers. Beyond maintaining current systems, making continued progress in research and development requires knowledge workers with an even deeper understanding of the sociocultural and technological systems at play.

Game-based learning is one approach to addressing these three recommendations. A variety of educational games around topics in cybersecurity already exist, including online games for children, digital training simulations, programming competitions, and analog games. We are interested in identifying the strengths of current approaches with the explicit goal of identifying new opportunities. That is, we believe that if we understand cybersecurity and what learning outcomes are supported by current generation educational games, then we can identify pragmatic approaches for developing next-generation solutions.

This work focuses on games for youth around ages 12–16. These are formative years in which individuals' perspectives about careers and technology are formed (see Margolis and Fisher [2], for example). Potential players in this age range are usually ingrained in rigorous formal and informal learning environments, and so there are opportunities to incorporate interventions around the *Concepts and Conceptual Understanding* and *Recruitment and Retention* recommendations. Game-based learning strategies could also address these recommendations with an older, adult population as well, but this is beyond the scope of our study.

II. Background and Related Work

A. Cybersecurity and Epistemology

The Cybersecurity Education Workshop report identifies the need for an epistemology of cybersecurity [1]. That is, promoting cybersecurity education benefits from a coherent definition of the term itself, as well as an articulation of what is known—or what is knowable—about it. A recent National Academies report identified both technical and sociocultural elements of cybersecurity [3]. Technical elements include computers, networks, and cryptography, and sociocultural elements include policies, trust, and social engineering. Kessler et al. [4] describe cybersecurity as a subset of information security, itself part of the larger domain of information assurance. They further recognize that cybersecurity is about process—not technology—and so a STEM (Science, Technology, Engineering, and Mathematics) perspective is insufficient. They assert that "our response to cyberrelated security challenges of the day are not solely about technical solutions but must also involve a myriad of related topics such as national defense,

978-1-4673-7921-2/15/$31.00 ©2015 IEEE

economics, sociology, political science, diplomacy, history, and many other social sciences" (p.36).

A similar conceptualization of cybersecurity is reified in the Computer Science Curricula 2013 (CS2013) recommendations, particularly the Information Assurance and Security (IAS) knowledge area [5]. The IAS area is unique among those in the report in that its topics are pervasive throughout the other knowledge areas: the recommendation includes only nine core areas that are strictly IAS, but 63.5 hours of IAS concepts are distributed among the other knowledge areas. The epistemology represented by this recommendation is particularly useful for our analysis due to the inclusion of both concepts and learning outcomes. The learning outcomes are further classified using a system inspired by Bloom's taxonomy of the cognitive domain [6] in which each objective marked with one of three levels of mastery—familiarity, usage, and assessment—which map roughly to Bloom's levels of understanding, application, and evaluation. It is worth noting that these recommendations are approved by a large panel of recognized experts across both the ACM and the IEEE. For these reasons, our own work uses these recommendations as a primary reference for cybersecurity epistemology.

B. Games and Learning

We approach games and learning from the perspective that games are rapid-feedback systems, and since timely and appropriate feedback is a necessary element for learning [7], [8], we see games essentially as teaching machines. Koster [9] describes how learning is an essential aspect of what we call "fun" in games. Built upon Csikszentmihalyi's concept of *flow* [10], Koster's Theory of Fun for Game Design argues that games teach players to overcome challenges, and "fun" arises from the balancing of skill and challenge. Swink [11] uses a similar argument from an aesthetic perspective, arguing that *game feel* comes in part from designing a game as a teaching system that produces, in players, both learning and a feeling of accomplishment.

The goal of formal educational systems is *transfer*—that what a student learns in one context can be applied in another. This is a particular challenge for games, where the learning is necessarily embedded within the formal and dramatic elements created by the designer. Linderoth [12] describes how the it is a matter of affordances, following the ecological model of perceptual learning [13]: to act meaningfully in the world requires the recognition of an affordance, the taking of an action, and the capacity to receive feedback on the action's impact. Consider *CyberCIEGE* [14] for example—one of the games that we reviewed that presents the user with a simulated work environment. The game affords learning about cybersecurity within the realistic yet simulated game world, where the operating systems, software products, people, and governments are abstract and fictional. A player may earn high scores in *CyberCIEGE*, but if the player cannot apply this learning outside of the game environment, then the product fails at its fundamental design goal.

A review of the literature revealed no scholarship evaluating the efficacy of existing cybersecurity education games. For most of the projects we evaluated, there is no mention of them in the literature whatsoever. Others, such as Irvine et al. [14], Twitchell [15], and Nagarajan et al. [16], justify their respective design decisions withing various theoretic models, but without the rigor of systematic evaluation or assessment data. While the authors claim to be following reasonable practices, these claims lack substantiation. While we agree with Stokes et al. [17] that it is divisive to claim any one definition of "impact," we remain concerned that many of these projects are taxpayer-supported and have produced no evidence of success or rigorous standards.

Good design practice, then, is essential, although this is one of few truths recognized among educational game designers. The draft report by Stokes et al. [17] describes the field as one of deepening silos and fragmentation, in part because of failure to recognize the various multidisciplinary and interdisciplinary perspectives that come together in this space. Klopfer et al. [18] survey the history of educational games and provide sound, research-based strategies for designers, and these strategies informed our analysis methods. These specifically address our first recommendation from the Cybersecurity Education Workshop report [1]; to address assessment, we turn to research-based approaches such as those described by Hickey [19] and Mitgutsch and Alvarado [20].

We note that the classification of learning objectives in CS2013—described in the previous section—are particularly applicable for the design of game-based learning environments. *Familiarity* can be included through a game's formal or dramatic elements. *Usage* manifests as actions the player can take—that is, these are the mechanics of the game, where one finds the game in the content [18]. *Assessment* represents a conceptual abstraction that requires extended abstract reasoning [21]. A game may encourage players to reach this level of understanding through clever mechanics design; however, this may also represent an opportunity for the use of debriefing as a post-play learning activity—an approach that has been shown to bring rich, higher-level learning results from game-based and simulation-based experiences [22]–[24].

Burgun's taxonomy of interactive forms [25] provides a useful framework from the context of game-based learning. His taxonomy identifies four forms: a system without goals is a *toy*; adding a goal yields a *puzzle*; further adding competition yields a *contest*; and finally, adding meaningful ambiguous decisions yields a *game*. It is important to note that his use of these terms is descriptive: he does not claim that all things called a "game" fit his taxonomy this way, but rather that what *he* calls a "game" is described as given—an approach that respects Wittgenstein's argument that the word cannot really be defined anyway [26]. Burgun's taxonomy is useful because it allows for an unambiguous classification of artifacts based on their designed properties: an interactive composed entirely of multiple-choice questions is a *puzzle* where the player attempts to pick the right answer. The learning value of such digital tests are limited compared to those that realistically embed a context into in-game experiences. For example, Hickey et al. [27] describe how incorporating real scientific inquiry into *Quest Atlantis*—thereby making it a *game* in Burgun's taxonomy - also increased the learning gains significantly.

III. Analysis

We focused our analysis on these research questions:

Q1 Does the game include cybersecurity content?

Q2 Do the game mechanisms directly support the learning objectives?

Q3 Does the game describe careers in cybersecurity?

Q4 Does the game explain educational paths toward careers in cybersecurity?

The first question was used as a sieve to identify what games we would consider for analysis. We acknowledge that there may be games that legitimately teach cybersecurity concepts despite not including it as a theme, this was beyond the scope of this work. The second question was used to allow us to more easily identify trends among similar games: by looking more critically at the game mechanisms, we can identify which follow the advice to find the game in the content. Specifically, we look for evidence that the game mechanisms are tied to authentic cybersecurity education learning outcomes [5], following Klopfer et al. [18] and Hickey [19]. To be clear, we mean "mechanisms" in the sense of formal elements—the game components with which a player directly interacts, as opposed to dramatic elements that frame the play experience [28]. The third and fourth questions tie explicitly to the *Recruitment and Retention* recommendation from the Cybersecurity Education Workshop report [1].

The specific games included in our analysis were chosen based on a combination of keyword searches on the Web, recommendations from cybersecurity professionals, and personal experience, and the games are listed in Table I. Although we focused on games designed explicitly to teach cybersecurity, we also selected other games that include cybersecurity themes: in particular, *Bioshock*, *Shadowrun Returns*, and two entries from the *Deus Ex* franchise were selected for their inclusion of "hacking" experiences. *Android: Netrunner* and *Control-Alt-Hack* were chosen as analog games based on cybersecurity themes, the latter having been designed as a teaching tool. *Capture the Flag* is one of many eponymous games in which teams of programmers simultaneously secure their own servers while hacking opposing teams' in a time-limited competition; we selected the implementation from Buena Vista University due to our ability to informally interview a team coach. We were unable to obtain research access to *NetWars* (SANS) and *CyberNEXS* [16] (Leidos), two commercial cybersecurity games. The evaluation of *CyberProtect* [29] was limited to analysis of a descriptive gameplay video, not first-hand experience.

These games we analyzed were designed for a wide range of target audiences. Some are clearly designed for young children and focus on encouraging simple safe online habits, whereas games such as *Capture the Flag* require specialized programming knowledge in order to minimally participate.

IV. Findings

Table I lists the games and provides a summary of our assessment, using a three-tier model described below. All of the games included cybersecurity content (Q1): as mentioned above, this was a criteria for their selection, although the nature of this inclusion varied. At one extreme, *CyberCIEGE* provides a simulation of a company with multiple networked computers, digital assets such as databases, workers who need training, policies that require enforcement, physical security, and technical components such as access control lists and password strength requirements [14]. At the other extreme is *Gem Jam!*, which starts with a static screen of online gaming tips and then proceeds as a *Bejeweled* (PopCap) clone with no other mention of cybersecurity content.

It is the investigation of our second research question—whether the game mechanics support the learning objectives—that led to our three-tier model indicated in Table I. These three tiers are:

Type 1 Games that convey cybersecurity concepts through narrative and/or theme only. There is no representation of the concepts within actual gameplay. That is, the act of playing the game does not require any decision-making that would reflect an understanding of cybersecurity concepts.

Type 2 Games that integrate multiple-choice questions (including yes/no options and branching narratives) that correspond to cybersecurity concepts. Answering these prompts correctly requires an understanding of the concepts.

Type 3 Games that require ambiguous decision-making such that making good decisions implies an understanding of cybersecurity concepts.

Type 1 Games

Type 1 games show minimal learning potential through gameplay: cybersecurity concepts are only present in narrative, but not through players' decision-making processes. The suite of games produced by the National Center for Missing & Exploited Children exemplifies this category. In *Stop That Post*, for example, the player is told that friends or family are going to post something embarrassing online, and that they must race to stop them. The player then plays a 2D physics-based platformer, and if successful, they receive narrative feedback that the social media post was prevented. Playing the platform game has nothing to do with cybersecurity content: one could easily click through the narrative, enjoy the game, and emerge none the wiser about safe online habits. The games we classify as Type 1 exemplify the phenomenon of narrative as a feedback mechanism, not a mechanism [30]; furthermore, they fail to capture the essential desired learning outcomes into gameplay, as best practices dictate [18].

This is not to say that these games have no value. Most of the games in this category were designed for young players, and the games are part of a rich ecology of content designed around themes of safe online habits. While the games may not teach through gameplay, they serve as incentive to bring young people to the site, where they can find other tips, videos, and activities that reinforce these ideas. This use of games-as-marketing is common in the commercial sector, and it is uplifting to see a beneficial organization such as the National Center for Missing & Exploited Children using it for positive social impact.

Control-Alt-Hack presents an interesting case for analysis. It is a game in which the players are white-hat hackers competing to become CEO of a security company [31]. The game is a re-themed version of Steve Jackson Games' *NinjaBurger*, in

TABLE I. SUMMARY OF GAME ANALYSIS

Title	Developer or Publisher	Type	Pedagogic Intent
Control-Alt-Hack	University of Washington	1	yes
Cyberbully Zombies Attack!	National Center for Missing & Exploited Children	1	yes
Gem Jam!	National Center for Missing & Exploited Children	1	yes
Inbox Defender	National Center for Missing & Exploited Children	1	yes
Password Plunder	National Center for Missing & Exploited Children	1	yes
Stop That Post	National Center for Missing & Exploited Children	1	yes
Tad's Profile Panic	National Center for Missing & Exploited Children	1	yes
Bioshock	2K Boston / 2K Australia	1	no
Deus Ex	Ion Storm	1	no
Shadowrun Returns	Harebrained Schemes	1	no
Cybersecure	HealthIT.gov	2	yes
Growing an Online Reputation	Carnegie Mellon University	2	yes
Mission: Laptop Security	OnGuardOnline.gov	2	yes
Phishing Scams	OnGuardOnline.gov	2	yes
Safe Online Surfing	FBI	2	yes
Capture the Flag	Buena Vista University	3	yes
picoCTF	Plaid Parliament of Pwning and Team Daedalus	3	yes
CyberCIEGE	Naval Postgraduate School	3	yes
CyberProtect	Carney, Inc.	3	yes
Cybersecurity Lab	NOVA Labs	3	yes
Android: Netrunner	Fantasy Flight Games	3	no
Deus Ex: Human Revolution	Eidos Montreal	3	no

which the players are ninja fast-food delivery agents who are competing to take over the franchise. The mechanisms of the game are identical: the player accomplishes missions by rolling dice and comparing the results to various skills. The five skills in *NinjaBurger* are combat, stealth, disguise, climbing, and customer service; these become hardware hacking, software wizardry, network ninja, social engineering, and cryptanalysis in *Control-Alt-Hack*. In either case, the gameplay does not involve stealth, disguise, software wizardry, or cryptanalysis: the player rolls dice and compares them to a skill's numeric value. To claim that *Control-Alt-Hack* teaches about cybersecurity, then, is an equivalent claim that *NinjaBurger* teaches about ninjitsu and fast food. Both games incorporate tactical risk management, but this is not tied intrinsically to their content domain. Without empirical data or established theoretical models of educational game design, claims about what the game teaches are unfounded. By contrast, consider TiltFactor Labs' *Buffalo*, a card game designed to overcome personal biases, which was designed following best practices of transformative game design, and which has been shown to have significant cognitive effects [32].

Given that Type 1 games do not incorporate key concepts into the gameplay, but we have already established that all games teach something, there is a possibility that these games are working against their stated goals. In the absence of evidence or models, we are left with the distinct possibility that playing one of these games may cause the player to build inaccurate mental models about cybersecurity. For example, the dice-based risk management of *Control-Alt-Hack* could result in a player thinking that online risks are worth taking, or *Stop that Post* may make the player believe that they can remotely police their friends' and families' social media habits.

Type 2 Games

The emergence of this classification came from the observation that many of these "games" are essentially interactive digital quizzes. That is, the gameplay consists of viewing prompts and selecting from a list of options; these are *puzzles* in Burgun's taxonomy [25] since they have pre-ordained best solutions. Just like any other multiple choice exam, such games could be used as assessments of learning, but only if the constructed items are reliable and valid. These games can also be used as self-paced replacements for traditional educational interventions. They certainly don't capture the essence of "finding the game in the content." Although a cybersecurity professional does frequently read and make decisions, these decisions are rarely as constrained as two to four options in a game.

A strength of games in this category lies in their ability to teach through narrative. Games such as *Mission: Laptop Security* tell an interesting story about a protagonist spy who previously lost a laptop and now is subject to institutional oversight; the choices in *Cybersecure* are based on realistic and compelling scenarios from health information technology. These are not teaching through gameplay, in the sense we have approached it, but through narrative; a story-based learning evaluation model is more appropriate to apply than a games-oriented one.

As a clarification, note that *Safe Online Surfing*—which we classified as Type 2—is actually a suite of games targeting U.S. grades 3–8. Each grade level includes eight minigames. Some of these fit into our Type 2 classification, while others are Type 1: they are cybersecurity-themed minigames where the core gameplay has no relationship to the content. We have classified the entire suite as Type 2 since they are offered as one product.

Type 3 Games

Type 3 captures *game* in the sense defined by Burgun [25]: a competition that involves endogenously meaningful ambiguous decision-making. These are not puzzles with single solutions, and hence, they represent opportunities for extended learning through repeated play.

The most illustrative example is *Cybersecurity Lab*, which takes three minigames and threads them together into a compelling cybersecurity narrative. The three minigames are designed around authentic, though abstract, cybersecurity learning objectives. One is a scaffolded series of puzzles in which the player must make strong passwords and guess an opponent's; the player can observe that the opponent can more easily guess simpler passwords as compared to more complex one. A second minigame involves identifying phishing scams by comparing real and fraudulent communications (within the fictional world). The third minigame develops computational thinking skills [33] by using a blocks programming language—as in *Scratch* [34] and *App Inventor* [35]—to program solutions to mazes. These minigames clearly make the content into a game and represent good practices for educational game design [18]. Furthermore, they are embedded into a Web context that includes additional media to explain careers in cybersecurity. Like the Type 1 games, *Cybersecurity Lab* provides an engaging play experience that brings players to an informational portal, but more impressively, the game itself manifests good design principles.

Whereas *Cybersecurity Lab* is an abstraction of cybersecurity concepts appropriate for younger children, *CyberCIEGE* exemplifies the opportunities in a simulation game. As mentioned above, *CyberCIEGE* involves making tactical decisions about financial allocation, with options including hardware acquisition, network configuration, personnel training, policy enforcement, and physical security. These are relevant decisions for cybersecurity content, albeit in a fictionalized environment.

A weakness of *CyberCIEGE*, *Cybersecurity Lab*, and others is that the player decisions are against discrete, algorithmic opponents: that is, each of these is really an elaborate *puzzle* that has a best solution [25]. By contrast, *Capture the Flag* has players directly engaged in real cybersecurity challenges against opposing teams. They must work together to identify vulnerabilities and protect against them, and when making offensive moves, they try to circumvent the protections installed by opponents. The technical elements of cybersecurity content are deeply embedded in this game, but it comes with a high price of admission: players must already be competent computer programmers and savvy with computer system operation. While this population is prime for recruitment into cybersecurity careers, targeting them does little to improve the overall pipeline, much less issues such as diversity [2].

It is important to consider what players can learn from the games that are not designed to teach cybersecurity. In the original *Deus Ex*, "hacking" was merely a matter of spending the right resources and having limited time to gather information from computer consoles. The subsequent *Deus Ex: Human Revolution* revised this to a minigame involving connecting to multiple servers across a network topology without being traced. The first is a poor abstraction of cybersecurity, while the latter includes some relevant game mechanics and theme. *Shadowrun Returns* includes lengthy sequences in which characters plug into "the Matrix" and enter a cyberpunk-style virtual world of avatars battling intruder countermeasures. The Matrix levels follow a similar geography to the non-Matrix levels, and it still essentially a strategic combat simulator of ranged and melee combat: the character attributes and abilities are different, but the fundamental mechanics are those of tactical turn-based combat, which do not significantly represent cybersecurity fundamentals. *Android: Netrunner* also features a dystopian cyberpunk theme, but it is more coherently situated within authentic cybersecurity themes. It is an asymmetric game, with one player taking the role of the corporations and the other, the "runner"; the corporation wins by advancing agendas that are hidden across servers, while the runner wins by stealing these agendas through hacking. That is, the mechanics involve secret information, defenses against unpredictable attackers, and different goals for each side, all of these being authentic cybersecurity topics. Of course, elements of this game also violate reality: we have no countermeasures that literally fry the brains of opposing hackers. Further study is necessary to determine what people learn about cybersecurity by playing these games—both accurate and inaccurate learning—and this points again to the value of post-play debriefing as a means for helping players form useful mental models [22]–[24].

Realism vs. Dehumanization

Many of the children's games included cyberbullies as a narrative element, and these were consistently portrayed as subhuman or nonhuman. *CyberBully Zombie Attack!* is a tower defense game in which the player defends a school from "cyberbully zombies." *Safe Online Surfing* includes a challenge against a cyberbully pirate crab who needs to be stopped before he sends a mean email. This design decision has a distinct othering effect. By portraying cyberbullies as something inhuman and evil, it fails to reflect the reality that there is someone else on the other side of the computer with their own motives and story, simultaneously a more difficult and more important reality to portray. We are concerned that this may be insulting to those students who have dealt with the harsh realities of cyberbullying, as indicated by some of our informal interviews.

Other games portray the conflict between opposing sides more evently. *Android: Netrunner* presents a fictional world with two playable sides: that of a corporation and that of hacker. Netrunner creates a unique set of motives and objectives for each side and thus humanizes each position, albeit within a cyberpunk aesthetic. Despite the fictional theme, the game narrative captures the notion that the corporations have information that they must secure in clever ways, and they must do so purely through predictive defenses, while solitary individuals with a network connection can potentially break in and steal sensitive information. *Capture the Flag* takes a different approach: all of the teams are engaged in a friendly competition, and each is taking both offensive and defensive maneuvers. By doing so, the players learn how to harden systems and how to think like attackers; the unstated assumption is that the players will use this knowledge for social good and not for criminal or nefarious purposes. These games foster a richness of perspective that relates to non-game reality, rather than simple demonization of the enemy. As Koster [9] describes, demonization of the enemy may be a common game storytelling technique, but it does not represent 21st-century values.

V. Conclusions and Future Work

Evaluating cybersecurity education games based on their design characteristics produced a three-tier taxonomy. We observe significant variability among the games regarding the integration of cybersecurity education learning objectives into gameplay mechanisms, and the literature suggests that those with better integration should produce better learning outcomes. However, we discovered no empirical assessments of any of these projects, and very few articles explaining, contextualizing, or justifying their designs. This is problematic for cybersecurity education, and we are concerned that federally-funded projects are not producing appropriate scholarship to advance the field. Not only does the community not know which techniques are efficacious for what purposes, but we also do not know if the games themselves are producing learning outcomes contrary to their stated goals.

Our analysis demonstrates the value of investigating both digital and non-digital games, as well as those not designed for pedagogic purposes. Such games can produce authentic learning outcomes, and many of those we evaluated have much further reach than any of the digital, pedagogically-designed games. These can be combined with educational interventions such as inquiry-based investigations and debriefing sessions to help learners contextualize what they have learned and transfer it to other situations.

There is an opportunity to create games based around careers and educational paths toward careers in cybersecurity. This relates to a specific recommendation from the Cybersecurity Education Workshop [1]. Although some existing games address these issues with ancillary content such as collocated videos and text, these are not addressed directly in any of the games we reviewed. It is not the goal of this work to provide requirements for specific educational game designs, but rather a useful lens through which to consider the designs themselves. The requirements for individual games will depend on context-specific factors such as the intended audience, environment of play, and development budget.

The games with the most authentic portrayal of cybersecurity content are also those with the highest barriers to entry. That is, there are broadly accessible games with little or no mechanisms for teaching cybersecurity concepts, and there are simulation games that require specialized understanding of technical skills or understanding of information systems and their management. *Cybersecurity Lab* is the only game we reviewed that seems to scaffold a learner between these two levels, and so we believe there is an opportunity here as well for new projects and initiatives.

Acknowledgment

This research is based upon work supported by the National Science Foundation under Grant No. 0968959.

References

[1] "Cybersecurity education workshop: Final report," https://research.gwu.edu/sites/research.gwu.edu/files/downloads/CEW_FinalReport_040714.pdf, Feb. 2014.

[2] J. Margolis and A. Fisher, *Unlocking the clubhouse: Women in computing*. Cambridge, MA, USA: MIT Press, 2003.

[3] D. Clark, T. Berson, and H. S. Lin, Eds., *At the nexus of cybersecurity and public policy: some basic concepts and issues*. Washington, DC, USA: The National Academies Press, 2014.

[4] G. C. Kessler and J. Ramsay, "Paradigms for cybersecurity education in a homeland security program," *Journal of Homeland Security Education*, vol. 2, p. 35, 2013.

[5] ACM/IEEE-CS Joint Task Force on Computing Curricula, "Computer science curricula 2013," ACM Press and IEEE Computer Society Press, Tech. Rep., December 2013.

[6] B. S. Bloom, M. D. Engelhart, E. J. Furst, W. H. Hill, and D. R. Krathwohl, *Taxonomy of educational objectives: The classification of educational goals. Handbook I: Cognitive domain*. New York: David McKay Company, 1956.

[7] S. A. Ambrose, M. W. Bridges, M. DiPietro, M. C. Lovett, and M. K. Norman, *How Learning Works: Seven Research-Based Principles for Smart Teaching*. San Francisco, CA, USA: Jossey-Bass, 2010.

[8] J. Hattie and G. Yates, *Visible Learning and the Science of How We Learn*. London, UK: Routledge, 2013.

[9] R. Koster, *A Theory of Fun for Game Design*. Phoenix, AZ: Paraglyph Press, 2004.

[10] M. Csikszentmihalyi and M. Csikzentmihaly, *Flow: The psychology of optimal experience*. HarperPerennial New York, 1991, vol. 41.

[11] S. Swink, *Game Feel: A Game Designer's Guide to Virtual Sensation*. Boca Raton: CRC Press, 2009.

[12] J. Linderoth, "Why gamers don't learn more. an ecological approach to games as learning environments," in *Proceedings of DiGRA Nordic 2010: Experiencing Games: Games, Play, and Players*, L. Petri, T. A. Mette, V. Harko, and W. Annika, Eds. Digital Games Research Association, 2010.

[13] J. J. Gibson, "The Theory of Affordances," in *Perceiving, Acting, and Knowing: Toward an Ecological Psychology*, R. Shaw and J. Bransford, Eds. New Jersey: Lawrence Erlbaum, 1977, pp. 67–82.

[14] C. E. Irvine, M. F. Thompson, and K. Allen, "Cyberciege: gaming for information assurance," *Security & Privacy, IEEE*, vol. 3, no. 3, pp. 61–64, 2005.

[15] D. P. Twitchell, "Securitycom: a multi-player game for researching and teaching information security teams," *Journal of Digital Forensics, Security and Law*, vol. 2, no. 4, pp. 9–18, 2007.

[16] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," in *Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), 2012 IEEE International Conference on*. IEEE, 2012, pp. 256–262.

[17] B. Stokes, N. Walden, G. O'Shea, F. Nasso, G. Mariutto, and A. Burak, "Impact with games: A fragmented field," Games for Change, Pittsburgh, Tech. Rep., 2015, http://gameimpact.net/reports/fragmented-field.

[18] E. Klopfer, S. Osterweil, and K. Salen, "Moving learning games forward: Obstacles, opportunities, & openness," The Education Arcade, MIT, Tech. Rep., 2009, http://education.mit.edu/papers/MovingLearningGamesForward_EdArcade.pdf.

[19] D. T. Hickey, "Participatory assessment: A game design model for impacting engagement, understanding, and (as necessary) achievement," in *GLS 9.0 Proceedings*, C. C. Williams, A. Ochsner, J. Dietmeier, and C. Steinkuehler, Eds. Pittsburgh, PA, USA: ETC Press, 2013, pp. 175–181.

[20] K. Mitgutsch and N. Alvarado, "Purposeful by design?: a serious game design assessment framework," in *Proceedings of the International Conference on the Foundations of Digital Games*. New York, NY, USA: ACM, 2012, pp. 121–128.

[21] K. Collis and J. Biggs, *Evaluating the quality of learning: The SOLO Taxonomy*. New York: Academic Press, 1986.

[22] M. Pearson and D. Smith, "Debriefing in experience-based learning," *Reflection: Turning experience into learning*, pp. 69–84, 1985.

[23] R. M. Fanning and D. M. Gaba, "The role of debriefing in simulation-based learning," *Simulation in healthcare*, vol. 2, no. 2, pp. 115–125, 2007.

[24] S. Nicholson, "Completing the experience: Debriefing in experiential educational games," in *Proceedings of The 3rd International Conference on Society and Information Technologies*. Winter Garden, FL, USA:

International Institute of Informatics and Systematics, 2012, pp. 117–121.

[25] K. Burgun, *Game Design Theory: A New Philosophy for Understanding Games*. Boca Raton: CRC Press, 2012.

[26] L. Wittgenstein, *Philosophical Investigations*. Oxford: Blackwell Publishing, 1953.

[27] D. T. Hickey, A. A. Ingram-Goble, and E. M. Jameson, "Designing assessments and assessing designs in virtual educational environments," *Journal of Science Education and Technology*, vol. 18, no. 2, pp. 187–208, 2009.

[28] T. Fullerton, *Game Design Workshop: A Playcentric Approach to Creating Innovative Games*. Boca Raton: CRC Press, 2008.

[29] "*CyberProtect*."

[30] R. Koster, "Narrative is not a game mechanic," Jan. 2012, http://www.raphkoster.com/2012/01/20/narrative-is-not-a-game-mechanic.

[31] T. Denning, T. Kohno, and A. Shostack, "*Control-Alt-Hack*: A card game for computer security outreach, education, and fun," Department of Computer Science and Engineering, University of Washington, Tech. Rep. UW-CSE-12-07-01, 2012.

[32] G. F. Kauffman and L. K. Libby, "Changing believes and behavior through experience-taking," *Journal of Personality and Social Psychology*, vol. 103, no. 1, pp. 1–19, 2012.

[33] J. M. Wing, "Computational thinking," *Communications of the ACM*, vol. 49, no. 3, pp. 33–35, 2006.

[34] M. Resnick, J. Maloney, A. Monroy-Hernández, N. Rusk, E. Eastmond, K. Brennan, A. Millner, E. Rosenbaum, J. Silver, B. Silverman *et al.*, "Scratch: programming for all," *Communications of the ACM*, vol. 52, no. 11, pp. 60–67, 2009.

[35] E. Spertus, M. L. Chang, P. Gestwicki, and D. Wolber, "Novel approaches to cs 0 with app inventor for android," in *Proceedings of the 41st ACM technical symposium on Computer science education*. ACM, 2010, pp. 325–326.

Author Biography

Paul Gestwicki is an Associate Professor in the Computer Science Department at Ball State University. He teaches multidisciplinary undergraduate teams in an academic studio, mentoring them in the creation of original educational video games.

Kaleb Stumbaugh is an undergraduate research assistant at Ball State University. He is majoring in Computer Science.