Educational Design Research for the Development of a Collectible Card Game for Cybersecurity Learning

Michael K. Thomas¹ · Andria Shyjka² · Skip Kumm³ · Rigel Gjomemo⁴

Published online: 20 March 2019
© The Author(s) 2019

Abstract

The purpose of this paper is to explore the notion of formative design in the context of the design, development, implementation, and evaluation of a collectible card game (CCG) for teaching cybersecurity to middle school students. The approach involved a formative design approach, educational design research (EDR) that evolved from design-based research and design experiments commonly employed in fields such as the learning sciences, educational technology, and instructional design. The authors assert that the EDR process used to design an educational CCG is an effective approach for formative learning game design work.

Keywords Cybersecurity · Educational design research · Design based research · Collectible card games

The information age has an Achilles heel. Governments and enterprise organizations greatly rely upon computer systems and networks for their ability to exchange information and support decision processes. However, this digital infrastructure is also vulnerable to attacks by criminals, foreign nations, hackers, and disgruntled employees. In 2015, the Government Accountability Office reported that the number of security incidents related to federal agencies increased from approximately 5503 in 2006 to 67,168 in 2014, a more than tenfold increase (Wilshusen 2015). A recent annual analysis by the Ponemon Institute of 245 companies in seven countries found that the average cost of cybercrime to a company was \$11.7 million per year, with a maximum cost of over \$77.1 million (Ponemon Institute 2017).

Cybersecurity attacks have become a common occurrence causing profound damage. As we become more reliant on

cyberinfrastructure, we also become more vulnerable to cyberattack. While in office, President Barack Obama identified cybersecurity as one of the USA's most serious economic and national security challenges, but one that we are not adequately prepared to counter (Obama 2014). Shortly after taking office, President Obama ordered a review of federal efforts to deal with the problem of defending the US information infrastructure and to develop a comprehensive approach for meeting current and future cybersecurity threats (United States Department of Homeland Security 2011; United States Executive Office of the President 2011). In 2015, President Obama emphasized the importance of not only dealing with cybersecurity threats but also focusing on protecting children as part of this effort. He stated, "No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids" (Obama 2015).

The events surrounding the 2016 US presidential election demonstrate the urgent need for the development of cybersecurity expertise and for better and stronger cybersecurity systems. On May 11, 2017, President Trump issued an executive order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," which included a call for various sectors of the government to: "...assess the scope and sufficiency of efforts to educate and train the American cybersecurity workforce of the future, including **cybersecurity-related education** [emphasis added] curricula, training, and apprenticeship programs, from primary through higher education [emphasis added]" (Trump 2017)."

✉ Michael K. Thomas
micthom@uic.edu

¹ Department of Educational Psychology, University of Illinois, 1040 W. Harrison St. (MC 147), Chicago, IL 60607, USA

² Department of Educational Policy Studies, University of Illinois, Chicago, IL, USA

³ Department of Special Education, University of Illinois, Chicago, IL, USA

⁴ Department of Computer Science, University of Illinois, Chicago, IL, USA

The Nature of Cybersecurity

To aid in the development of the next generation of cybersecurity experts in the USA, educators need to increase students' knowledge of cybersecurity and their enthusiasm for pursuing a career in cybersecurity. Educators can do this by providing young students with opportunities that allow them to experience the habits of mind and habitual actions of cybersecurity professionals in developmentally appropriate, highly motivating, and accurate ways. To help prepare the next generation of cybersecurity experts, educators must consider the nature of cybersecurity work. According to the National Initiative for Cybersecurity Careers and Studies (NICCS 2015), cybersecurity professionals must possess particular skills. These include (1) agility—the ability to shift between roles or needs should a threat warrant different support, (2) multifunctionality—the ability to maintain and execute a variety of activities at any given time, (3) dynamism—the ability to provide for constant learning to effectively approach new endeavors and problems, (4) flexibility—the ability to move into new roles or environments quickly to increase knowledge and skills, and (5) informality—the ability to work in a nontraditional environment (NICCS 2015).

Additionally, cybersecurity professionals must be able to function in a fast-paced work environment, adapt to frequent and sudden changes in workflow, and manage emergent, highly complex problems using carefully managed resources. In general, the work of cybersecurity is opponent based; it involves “white hat/black hat, spy vs. spy” thinking. Cybersecurity professionals must be able to make decisions quickly in response to active opponents who are, in turn, trying to outwit them. This means that professionals new to the field must learn about how different “sides” think in a complex, continually evolving and game-like field of action. They must learn how to creatively “hack” and defend against the “hack” in ethical and thoughtful ways (Banks 2015). The work of cybersecurity also involves using an array of tools that are interrelated and are shared in cooperative affinity groups (Gee 2003) or communities of practice (Lave and Wenger 1991).

Teaching Cybersecurity To increase the pipeline of students interested in pursuing a career in cybersecurity, it is important to introduce them to the field before they enter high school so that they can then begin to select classes that will allow them to obtain the required skills. One challenge to this approach is to create a developmentally appropriate curricular experience that can both introduce middle school students to cybersecurity and help teach some of the habits of mind needed by cybersecurity professionals. Another challenge is to ensure that there is ease of access to the tools where more expensive options might leave those who do not have the funds unable to engage. One potential answer is to avoid the expense of creating fully immersive

computer-based cybersecurity simulations and instead allowing students to engage in real-time simulations that leverage activities in a developmentally appropriate analogical format. An opponent-based card game could simulate this experience by requiring players to work against one another using an interrelated complex array of skills. There should be attacks and defenses that require groups of people to get together and “play” and share in an affinity group. The game should be fast-paced, involving quick decisions in a competitive field of action. Most importantly, a game such as this should introduce middle school students to the habits of mind and habitual actions of cybersecurity professionals early, before they lose interest and leak out of the pipeline.

The term “gamification,” first used by Nick Pelling in 2002, has become popular as non-game contexts attempt to take advantage of game characteristics to make them effective, motivating tools and learning environments, which in turn furthers serious academic interest in the use of games for learning (Barab et al. 2004, 2005; Marczewski 2013; Pelling 2011; Squire 2006, 2011). Schools too often use abstract learning tasks creating a culture of learning divorced from experience that is more authentic. “Many of the activities students undertake are simply not the activities of practitioners and would not make sense or be endorsed by the cultures to which they are attributed” (Brown et al. 1989, p. 34). When games are used for education, feedback is immediate and social. The players must re-probe and must then reflect on their original thoughts or hypotheses about how the game is played (Gee 2003). Gee (2003) states,

One good way to make people look stupid is to ask them to learn and think in terms of words and abstractions that they cannot connect in any useful way to images or situations in their embodied experiences in the world. Unfortunately, we regularly do this in schools (p. 76).

Games, on the other hand, invite learners to probe and develop strategies to win. Students must form hypotheses about how to play and when and how to use in-game resources.

Collectible Card Games to Teach Cybersecurity To maximize a game's potential, designers of games for learning must leverage the affordances of games that make them compelling learning experiences. The emergence of trading card games, specifically collectible card games (CCGs), provides an opportunity for educators to utilize games for learning. Typically, CCGs are games of strategy where players compete with one another using their own decks of cards, normally sold in random assortments and commonly traded among players. Over time, players interact in affinity groups to build more powerful decks to use in competitions against other players, who themselves make use of their self-designed decks. Upgrading,

combining, and trading individual cards are hallmarks of the genre. The decade of the 1990s saw an important change in the phenomenon of trading cards with the emergence and explosion in the popularity of CCGs.

On August 5, 1993, the Wizards of the Coast game company released what is thought to be the first CCG, *Magic: The Gathering*. The game was designed for opponents to battle one another using decks of cards they assembled or collected during down times at video games conventions. Inspired by fantasy genre games such as *Dungeons & Dragons*, *Magic: The Gathering* has become a staple of global popular culture and spawned a new medium for gameplay in the entertainment industry. The *Pokémon* franchise, which includes a CCG, is now the highest grossing media franchise, generating more money than even the *Star Wars* or *Harry Potter* franchises (Wikipedia 2017). Other examples of popular CCGs are *Yu-Gi-Oh!*, *Cardfight Vanguard*, and *Android Netrunner*.

Particularly among youth, CCGs have grown into a pervasive form of contemporary gameplay. Hasbro (2016), the company that distributes the largest CCG, *Magic: The Gathering*, claimed in its 2012 annual report that *Magic's* revenue was “growing more than 30% and marking the brand’s fourth consecutive year of 25% revenue growth or greater” (p. 3). In its 2016 report, they claimed that *Magic: The Gathering* “delivered its eighth consecutive year of revenue growth” (p. 4). The number of CCGs has been steadily increasing owing to relatively low production costs and their popularity as components of media mixes (Ito 2005) for TV shows such as *Yu-Gi-Oh!* or massively multiplayer online games such as *World of Warcraft*. According to Turkay et al. (2012), powerful aspects of CCGs include their ability to stimulate creativity, cognition, and logical reasoning and aid players in synthesizing knowledge and developing skills difficult to teach in classroom settings. CCGs often become digital collectible card games (DCCGs) affording them even greater ubiquity and impact. DCCGs may be played online using computers, smartphones, or tablets, and may be played using consoles such as Xbox or PlayStation. DCCG players outnumber physical CCG players thanks to greater accessibility. However, CCGs remain immensely popular, played by millions of middle school children all over the world, and are potentially a low-cost/low-tech entry into spaces that are economically resource challenged and provide the first step into CCG experiences. Furthermore, CCGs have all the characteristics of the type of game that would be appropriate for having middle school children experience the habits of mind and habitual actions of a variety of expertise domains.

With the increase in popularity of CCGs and other card games, researchers have explored how CCGs may be used for educational purposes. Turkay et al. (2012) studied how CCGs may be used to promote learning and found that CCGs encourage players to think analytically, develop empathy, design iteratively, and communicate. They are

motivational, social, and dynamic. They also encourage mistake-making as a way of learning. It may be that incorporating a CCG as a way of teaching and learning could impart many related skills to students in addition to expanded career knowledge (Turkay et al. 2012). Furthermore, Adinolf and Turkay (2011) explored three positive aspects of using card games as educational tools: (a) motivation, (b) social play dynamics and mechanics, and (c) external/non-play mechanics. Motivation is represented in the students wanting to play to win and in obtaining rare cards as a reward mechanism in schools. Students also learn through complex social interactions and observation while playing CCGs. Additionally, while playing CCGs, students reported they try to avoid making the same mistake twice and may learn to problem solve as they experience the game. Lastly, through the collection of cards, students develop an understanding of resource management.

Developing Educational Games

Design-Based Research The concept and approach of design research exist across various research fields. One commonly appearing in the field of education is design-based research (DBR). The DBR process is a methodological approach that utilizes collaborative partnerships and mixed methods in determining the design of programs, curricula, and interventions in real-life messy contexts (Barab and Kirshner 2001). It involves multiple iterations and collaborative partnerships between researchers and practitioners (Anderson and Shattuck 2012; Design-Based Research Collective 2003). Design-based research, also called design experiments, is an effective means for simultaneously conducting research on learning and design in authentic learning environments (Brown 1992; Brown and Campione 1996; Cobb et al. 2003; Collins 1992, 1999; Collins et al. (2004). In this way, design work is seen as inherently iterative (Branch and Merrill 2012) and focuses on the design and testing of a significant intervention (Amiel and Reeves 2008). Elements of programs are continually piloted, and findings from testing and evaluation are cycled back into the formative design and research process (Hoadley 2002; Reigeluth and Frick 1999). According to Amiel and Reeves (2008), the development of design principles should undergo a series of testing and refinement cycles.

“Data is collected systematically in order to re-define the problems, possible solutions, and the principles that might best address them. As data is re-examined and reflected upon, new designs are created and implemented, producing a continuous cycle of design-reflection-design. The outcomes of design-based research are a set

of design principles or guidelines derived empirically and richly described, which can be implemented by others interested in studying similar settings and concerns” (p. 35).

DBR and the design experiments of Brown (1992) used an iterative approach similar to those used by Reinking and Bradley (2008) and Newman (1990) under the monikers “formative experiments” and “formative research” respectively. In an effort to draw together these related approaches under a single umbrella, McKenney and Reeves (2014) put forth a generic model for conducting what they call educational design research.

Educational Design Research In their synthesis of existing models of educational design research (EDR), McKenney and Reeves (2018) offer a generic model for design research in the field of education (see Fig. 1 for a modified version). Due to the iterative nature of design research, they conceptualize the application in terms of differing cycle sizes. The model they presented represents one mesocycle, commonly thought of as the regulative cycle, within which there are three phases or microcycles, each with distinct aims and outcomes. Multiple iterations of mesocycles make up a macro-cycle that represents the full scope of the design research that results in a completed product or innovation.

McKenney and Reeves (2018) outline three general phases, or microcycles, in conducting EDR. The first microcycle in EDR is the analysis and exploration phase, which is concerned with problem exploration, practically and theoretically followed by problem definition. Following this, the design and construction microcycle focuses on taking into account what has been learned and applying this knowledge to construct a relevant and practical innovation to address the problem. The final microcycle, evaluation, and reflection use the data collected in phase two to evaluate the innovation’s design and identify implications related to theory. EDR, like DBR, is at its heart an iterative approach; therefore,

phases may be repeated multiple times in response to what occurs in the work of the project.

The Current Project: *CySEC Crucible*

The study described in this paper utilized an EDR (McKenney and Reeves 2014) framework to explore an effort at creating a CCG for the purpose of teaching cybersecurity to middle school students in after-school programs. The research project involved continually refining and thoroughly testing a collectible deck-building card game designed to teach children cybersecurity and computer science content, while also increasing their enthusiasm for a future in computer science related careers. The goal of developing *CySEC Crucible* (CySEC) was to encourage more pre-high school students to take computer science courses when they are in high school and thereby be more prepared for more complex computer science work in college. To do this, CySEC was designed to accord with the popular style of existing collectible card games. For instance, in the popular CCG *Magic: The Gathering*, players take on the role of an individual who manages wizards and the mythical resource, mana. Similarly, CySEC positions players as managers of hackers and the object of the game is to engage a series of tasks to successfully hack opponents while also successfully thwarting opponents’ attempts to do the same. The game is won when a player reduces all of their opponents’ hackers’ data to zero. Like many other CCGs, CySEC is a deck-building game where the cards’ abilities are displayed uniformly on each card (see Fig. 2).

In CySEC, players develop their own strategy for playing and winning games by selecting 40 cards from a total of 99 available in the game. In this way, players may choose from many different strategies and creatively solve the problems related to both offensive and defensive gameplay. Card selection models the habits of mind engaged by real-life computer hackers and cybersecurity professionals who must continually create new strategies to accomplish their goals. The main goal

Fig. 1 This modified figure represents the three mesocycles of the CySEC research project (McKenney and Reeves 2018, p. 78)

Fig. 2 Layout of a hacker card in the CySEC CCG. In its current state of development, the CySEC cybersecurity learning card game has 18 hacker cards featured here. Each hacker has strengths and weaknesses in terms of their skill and equipment

of the CySEC is to teach general security principles via current defense and attack scenarios and techniques which are mapped onto to the game mechanics. These scenarios and techniques include defenses, such as different types of firewalls (network and host-based) and the use of honeynets (Araujo et al. 2015). Also employed are encryption and decryption schemes and their relative strengths and weaknesses, fishing attacks, monitoring and patching, misplaced trust in default configurations, and incident response and forensics. The principle underlying the design of *CySEC* is providing a comprehensive and exciting learning experience related not only to cybersecurity but also to the computer science surrounding cybersecurity. To this end, the game includes several components and layers that support teachers:

1. Concrete elements and concepts about cybersecurity (e.g., What is malware? What is a firewall?)
2. Processes and strategies in which those elements participate (e.g., how to set up defenses and attacks and then deciding how to proceed)
3. Tradeoffs between those strategies
4. Programming (e.g., the main loop)
5. Computing resources (e.g., rigs)
6. Adversarial thinking (e.g., deck knowledge and deck building), which is the process related to anticipating an adversary's move.

The cards in *CySEC* are of different types. There are pure attack cards, supporting attack cards, pure defense cards, supporting defense cards, resource cards, general support

and game mechanics cards, instruction cards, and hacker cards. Players learn by playing the game as well as by preparing to play (see Figs. 3 and 4).

Methods

The *CySEC* research study demonstrates all the characteristics associated with EDR as outlined by McKenney and Reeves (2018), which we modified for the purpose of the *CySEC* research project (see Fig. 1). Our development of an educational product in the form of an opponent-based, cybersecurity card game addresses a pragmatic concern about America's sparse cyber workforce in a time of increasing demand (Bureau of Labor Statistics 2014). The development work required a high degree of collaboration due to the multidisciplinary aspects of computer science content, educational goals, and game design. Additionally, this project has been made up of several cycles of "design, development, testing and revision" (McKenney and Reeves 2014 p. 11). The goals of this project are both practical and academic in nature. Firstly, we seek to create an educational product that addresses an area of need. Secondly, we document the process of the product creation to serve as useful information and model for future multiple-disciplinary collaboration for creating effective educational games.

Through our initial needs assessment and context analysis conducted in the form of a systematic literature review, we identified a dearth of human capital to fill the growing employment demands of the cybersecurity sector. Additionally, it was evident that further support was needed to develop mechanisms to teach youth about cybersecurity concepts in a way

Fig. 3 In its current state of development, the CySEC cybersecurity learning card game has 18 hacker cards. Players “tick” through turns using the “main loop” cards (pictured in the lower row). Each hacker

has strengths and weaknesses in terms of their skill and equipment that may be augmented with resource cards. The functions of each element mirror real-life elements of computer science and cybersecurity content

that may encourage them to pursue the field later in life. Being that cybersecurity is adversarial in nature and that there is a current trend of gamification in education (Pelling 2011), this needs assessment in combination with current educational trends guided the researchers to engage in an EDR process.

This effort was aimed at creating an educational game that would introduce not only cybersecurity content but also the inherent nature of the opposition, attack, and defense, which characterizes the field. In following the EDR process, we sought to gain a robust understanding of the content, context,

Fig. 4 Resource, instruction, and software cards allow players to simulate different approaches to cybersecurity offense and defense

and culture of the activity of the project drawing upon design principles from existing literature sources and by interviewing experts in the field of cybersecurity and game design.

Educational Design Research—Three Mesocycles

After the research team conducted a needs analysis and the goals and research questions were established, we conducted several mesocycles of inquiry. The iterative process of EDR provided us with an appropriate framework to approach our inquiry during the construction of *CySEC*. Here we will present an accounting of the three EDR mesocycles briefly outlined above in an effort to inform others undertaking this formative design process to produce an educational product. The first EDR mesocycle began by interviewing subject matter experts in cybersecurity and experts in the design of games for learning. We also explored existing cybersecurity games in the CCG genre. The only battle card game specifically designed to teach cybersecurity that we found was *Cyber Threat Defender* (Center for Infrastructure Assurance and Security 2018). In the second mesocycle, we established an informal after-school club at which we played *Cyber Threat Defender* with middle school students. By doing this, we were able to get a sense of the stakeholders involved related to the school, the target group, the physical context, the organizational context, and the viability (McKenney and Reeves 2014) of using a card game to teach cybersecurity in a school in an after-school setting. The experiences of the after-school program, combined with interviews with game experts, game designers, and cybersecurity experts, allowed us to continue to refine the development of *CySEC*. We then tested an early version of the game during the third mesocycle. Taken together, these three cycles have not only facilitated the development of an educational CCG about cybersecurity but also provided us with useful guidance for other researchers engaging in the multi-disciplinary development of an educational product.

First Mesocycle The first iteration of the mesocycle began with the analysis and exploration phase, or microcycle, in which we conducted interviews with (a) professional game designers, (b) academics who study the use of games for learning, (c) cybersecurity specialists, and (d) frequent players of CCGs. After gaining an understanding of how a CCG might be used to teach cybersecurity, we began producing the first prototype of the game. The game emerged from our collaborations that included an experienced game designer and cybersecurity expert. Our interview analysis was guided by the methods of grounded theory that included open-coding,

memoing, and theoretical coding (Glaser and Strauss 1967; Glaser 1978, 1992, 1998).

After developing a nascent version of *CySEC*, the research team began the design and construction phase by playing *CySEC* extensively as part of the alpha testing process. Playing *CySEC* consisted of the game designer and researchers talking through instructions, asking questions, and smoothing out gameplay features. Both aspects of gameplay and card level characteristics (e.g., card capabilities) were updated to produce a version of the game that had smooth mechanics and cards that were realistic displays of their cybersecurity capabilities. These play sessions helped us to prepare a version of the game that would be ready for field testing with middle school children in our third mesocycle.

Questions emerged while playing *CySEC* that transitioned us to the evaluation and reflection phase. During these phases, we used various methods to assess our perceived knowledge of the gameplay and card specific aspects of the game. For instance, each researcher wrote their version of the instructions to the game to evaluate and reflect on their knowledge and how it affected gameplay. The researchers also analyzed the text instructions on each card to analyze how the verbiage could be updated to make the instructions more intuitive without taking away from their real-world implications. To do this, we sought comments from gamers, game designers, educators, and cybersecurity experts. Lastly, the research team played *Cyber Threat Defender* to further understand the gameplay mechanisms of cybersecurity CCGs.

Second Mesocycle The second EDR mesocycle was implemented at a Catholic middle school located in a large Midwestern city. The urban middle school environment provided an opportunity to immerse the research design in a contextual and cultural perspective unique to the needs of middle school students in a real educational environment. In this phase, researchers used information gleaned from the first mesocycle to explore, design, and evaluate a weekly after-school club to examine the instruction of a cybersecurity curriculum and the characteristics of gameplay in an after-school cybersecurity club. During these sessions, we chose to play *Cyber Threat Defender* instead of our nascent development of *CySEC* so that we could develop a sense of what middle school students thought about a game that was already developed. We also did numerous other activities during the club, including playing password complexity games, deconstructing computer equipment, and doing artwork related to cybersecurity conceptual themes that students would like to see included on cards. The purpose of this semester-long effort was to understand the context of implementation. Understanding context and culture are essential for doing

design work that is culturally relevant and developmentally appropriate.

The analysis and exploration microcycle was iteratively applied to both the development of cybersecurity knowledge and card play game through instruction and gameplay with middle school students. During the gameplay portion of the after-school program, the students played *Cyber Threat Defender* allowing the researchers and game developers insight into the functions of gameplay that intrigued middle school students. The researchers participated in the gameplay as active participants and interacted with the middle school students to ask questions for further insight.

The design and construction microcycle involved the design of a cogent cybersecurity curriculum aligned with the contextual and cultural considerations of urban middle school students, as well as feedback from the students on gameplay. During the design portion of this phase the development team taught the fundamentals of cybersecurity, such as firewalls, encryption, and phishing attacks. The students then learned how cards from *Cyber Threat Defender* are related to topics that were taught and continued gameplay with other students and developers. Evaluating and reflecting upon this phase allowed the research team to adjust gameplay mechanics for *CySEC*.

The knowledge gained through observations and interactions in the second mesocycle informed the development of *CySEC* by providing the research team with contextual experiences that revealed the following: (a) complexity is needed to maintain enthusiasm, and (b) a story is not essential to gain initial interest. Although the next mesocycle occurred in a different setting and the students had a more extensive knowledge base on cybersecurity and CCG gameplay, the information gleaned from this mesocycle allowed the development team to deliver the first phase of beta testing *CySEC*.

Third Mesocycle The third iteration of the EDR mesocycle was implemented in a private Montessori school located in a suburb of a large Midwestern city. Initial orientation with the student participants revealed important differences in the context and culture of the sites. These differences allowed for a unique, new approach to the project that focused more specifically on the collaborative analysis and exploration of the beta version of *CySEC*. On average, student participants at this site were more familiar with collectible card games and gameplay mechanics. Some students were deeply immersed in this culture and acted as supports for students less familiar to gameplay and related concepts. Similarly, students generally demonstrated a greater depth and breadth of knowledge about computers. As a result, far less conceptual knowledge and vocabulary were needed, which instructionally allowed for the focus to be on reflective gameplay and game development. Therefore, after the exploration and analysis microcycle, it was evident that in this mesocycle, our inquiry could be

focused on the understandability and playability of *CySEC* for middle school students with the aim of product improvement.

The design and construction phase of this cycle was highly collaborative between university team members and student participants. Students at this site were previously familiar with iterative design and elements of constructive critique. As a result, the university team members simply identified potential areas for examination and critique to focus student attention. These areas included game esthetics, rules, gameplay, and specific card content. After an initial presentation of a simplified approach to playing *CySEC*, students were given time for gameplay. Each session included opportunities for the students to provide comments, questions, and suggestions regarding areas of critique. Generally, sessions began with the presentation of new card designs and art upon which students provided feedback. This was followed by time for gameplay and further discussion and critique based on the gameplay experience. Throughout gameplay, researchers circulated among the students recording student comments and discussions which were often used to initiate the end of session discussions. Researchers also engaged directly in gameplay with students. During gameplay, students were encouraged to make notes and suggest changes to specific cards by writing directly on them. These acted as data artifacts which showed the iterative, often concurrent design and construction components of this phase. These discussion points during sessions allowed not only student feedback but also a dialog about proposed solutions. The feedback and solution suggestions from one session were used to shape the next iteration of the game that was played the following week. Some suggestions resulted in small changes to card content that were found to have large implications for gameplay in the following week. In this way, the design and construction phase were tightly coupled with the evaluation and reflection microcycle during this mesocycle.

The weekly discussions held at the end of the play sessions allowed issues to be identified and potential solutions suggested for testing and discussion the following week. Each week, students were asked to evaluate and reflect on any changes that had been implemented. Solutions which received positive feedback after implementation were kept while others were further revised or discarded. At times, issues with the game were identified but no clear solutions were presented and therefore were left for the research team to attend to after the school sessions completed. Nonetheless, through the collaborative process with students, significant changes and improvements to *CySEC* were achieved. These changes included several card specific changes that altered the strength or parameters under which a card operated. These changes often had larger implications for gameplay, especially concerning the pace of play. Additionally, meaningful changes to the layout of cards were achieved which facilitated visual clarity and

eased the gameplay process. For example, confusion about which type of cards could be played on a given tic or turn was solved through matching the color-coding of play cards to the home loop card during which they could be utilized. Not only did this clarify and expedite gameplay but it also provided visual prompting for students about upcoming turns and supported students who were less familiar with cybersecurity concepts.

As a result of the mesocycle and beta testing undertaken at the Montessori school development of *CySEC* as an enjoyable, playable game and teaching tool were moved significantly forward. Consistent, directed student engagement in the design, construction, evaluation and reflection phases of the EDR process identified problems, surfaced preferences, and presented solutions for testing.

Demonstrative Example To demonstrate the EDR process and the role of multiple constituencies in the development of the *CySEC* educational card game, it is helpful to examine how a single game component evolved throughout the process. One software daemon card, *CorrectHorseBatteryStaple*, was initially designed to make a hacker immune to data loss through encryption, in this case, a level four encryption. The game designer was inspired to create this strong defense card based on an xkcd.com comic about how to make a strong password, which suggests the level of password complexity needed to protect accounts. Therefore, the game designer created this card to show that breaking encryption is an incredibly slow process, stating, “this is one of the reasons I made the input and output penalty so big here is because I really want it to be a trade-off between really good security in terms of encryption and being able to do things quickly if you’re using good passwords.” In reviewing the initial game design, a cybersecurity expert who was interviewed in the first mesocycle of this research project immediately recognized the card name as that of a website for generating secure passwords and defined the teaching element of the card as essential for teaching the “importance of having robust passwords.” The identification of the purpose of this card demonstrates a point of alignment between two constituencies, which was later challenged by a third constituency, the student players. During our third mesocycle, students played the beta version of the *CySEC* game and almost immediately vocalized concerns that some cards are too strong and inhibited the pace of the game, and therefore their enjoyment of *CySEC*. One student reported that the *CorrectHorseBatteryStaple* “is too overpowered” and many others agreed. When designing a learning game, it is essential to create a game that accurately not only teaches content but also is engaging and enjoyable so that students want to play the game. Therefore, the research team discussed the trade-offs and decided to reduce the power of the card to an encryption power of two. Following this decision, the researchers returned to the school and had the students play with

the altered card power. They acknowledged that while the encryption was still difficult to overcome, it was not to the level that it would deter them from playing the game. Through negotiating between the thoughts and opinion of our constituencies, we revised the game in a way that the learning goal was largely maintained but not at the cost of the enjoyment of the game (see Fig. 5).

Results and Discussion

As an EDR project, the design of the *CySEC* game was itself the result of the study. As such, we see the work of both the research and the design as ongoing. The design work continues to inform what we know about teaching and learning cybersecurity content for middle school children. It also informs what we know about the notion of formative design. Three major findings are summarized below.

Honoring Diverse Constituencies

Making an educational game requires input from multiple constituencies. For this project, it was essential that we incorporated the voices, critiques, and substantive input from (a) content specialists in the fields of cybersecurity and computer science. We had to make sure that the nomenclature, language, game mechanic, and image symbolism accorded with genuine content. It was also critical to incorporate the perspectives of (b) educators who grasped the subtleties of creating a curriculum for the game using cybersecurity content from the subject matter experts. We found differing cultures, content knowledge, skills, and desires operating in different contexts. Because this is a game of a particular type, it was necessary to understand the perspective of professional game designers who have experience creating collectible, deck-building card games. Finally, it was important to extensively test and bring in the voices of those for whom the game was designed. We had to have (c) game players in general, and middle school children in particular continually play the game and offer feedback on all aspects of the game and its design.

Identifying Tensions

A second important finding is that we managed to identify tensions inherent in the formative design of a game for learning. We found that the first of these tensions was that communication must be facilitated between the aforementioned constituencies. We found that these constituencies simply do not share a common language. There were different cultural proclivities and “folkways” among these three groups. Cybersecurity experts, for example, are not accustomed to speaking with educators. Similarly, game designers are not

Fig. 5 The evolution of the CorrectHorseBatteryStaple card

accustomed to working with educators and middle school children are not used to speaking with game designers. The second of these tensions is the chocolate covered broccoli problem, which is that while we want games to be fun and engaging, we also want students to learn, and we do not want these to be mutually exclusive. We consider that this will be a tension inherent in the formative design of educational games. Finally, we found that there is an inherent tension in implementing EDR in schools with students. Schools are complex organizations steeped in rules and tradition. In this project, we benefited greatly from having a school insider who was both working on the project and who previously taught at one of the schools with which we partnered. Having a person who knows the language and culture of the school facilitated the entire project. Cultivating such relationships is an inherent tension in the EDR process.

Mapping EDR Mesocycles in Formative Design

We found that the mesocycle model of McKenney and Reeves (2018) mapped onto the work we did. Specifically, microcycles 2 and 3 often worked in cyclical or tandem fashion during our weekly work with the children. We would recommend that designers in the field doing work in educational games make use of this model to guide the complexities of similar projects.

Limitations

Although the iterative EDR process employed in this study provided valuable knowledge related to the development of *CySEC*, there were several limitations. First, there is still a lack of robust data on the effectiveness of the *CySEC* game to increase cybersecurity knowledge or enthusiasm for pursuing cybersecurity as a career. Additionally, the initial development, alpha, and beta testing all included small sample sizes. The interviews with experts and initial testing involved 10 people, and the middle school gameplay experience included approximately 25 students. Additionally, the two middle school gameplay settings included two schools with students with varying background knowledge related to cybersecurity principles and CCG gameplay knowledge. The fully developed *CySEC* game needs to be played with a larger group of middle school students and data need to be collected on the efficacy of the game to attain its desired results. We are currently engaged in expanding the project to obtain the statistical power necessary to scientifically prove effectiveness.

Implications for Future Research

The *CySEC* project consisted of three EDR mesocycles that corresponded with initial development, alpha testing, and beta testing, which were all developmental in nature. Therefore,

additional EDR mesocycles are required that are evaluative and provide insight into the efficacy of using CCGs; specifically, *CySEC* establishing the validity of CCGs to increase middle school students' knowledge and enthusiasm for cybersecurity is an important next step in our research. Future game developers and researchers can implement qualitative and quantitative research methods to determine the effectiveness of *CySEC* as an educational gameplay intervention and as a part of an integrative experience embedded in a middle school cybersecurity curriculum. Future qualitative research could investigate students' excitement for the game and further analyze how they perceive the interactive gaming experience as it relates to cybersecurity. Additionally, quantitative research could explore the cybersecurity knowledge of middle school students and their knowledge related to the types of cybersecurity career options they can pursue and the required academic and training needed to obtain those positions. Further research should also be conducted to find ways to incorporate populations typically less involved cybersecurity career fields, such as minorities and women. Though our sample size was small, discussions between the research team and the middle school students during gameplay and formal interviews revealed that students expressed interest in continuing to learn about cybersecurity. Several students also stated that they enjoyed playing the game outside of the after-school club and enjoyed showing that they were cybersecurity "experts." Therefore, the *CySEC* research project could help address the nation's need to recruit more people to enter the cybersecurity career field, but additional research is needed to quantify students' interest in pursuing cybersecurity as a career. To do this, future research could focus on providing pre- and post-interviews and Likert scale assessments to determine if playing *CySEC* results in students enrolling in more cybersecurity courses in high school and increases students' excitement about a future cybersecurity career.

Conclusion

The goal of the *CySEC* project was to develop a CCG that middle school teachers could use as part of a cybersecurity curriculum to provide students with an opportunity to have an interactive cybersecurity experience, which reflects the realities of cybersecurity work. Through three iterative cycles of the EDR mesocycle, the *CySEC* game designers were able to obtain valuable input from cybersecurity experts, game designers, middle school students, and educational experts, to develop an interactive CCG that has the potential be incorporated in a school curriculum. The results of the *CySEC* EDR project, including interviews and gameplay with students, indicate that a CCG may be an effective approach to increase middle school students' interest in cybersecurity as a career field, as well as improving their knowledge related to cybersecurity. However, the *CySEC*-iterative EDR process is only

the first step in developing and testing a CCG that can both increase middle school students' interest in pursuing a career in cybersecurity while increasing their content knowledge about computer science and cybersecurity.

Compliance with Ethical Standards

Conflict of Interest The authors declare that they have no conflict of interest.

Open Access This article is distributed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>), which permits unrestricted use, distribution, and reproduction in any medium, provided you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license, and indicate if changes were made.

References

- Adinolf, S., & Turkay, S. (2011). Collection, creation and community: a discussion on collectible card games. In *Proceedings of the 7th International Conference on Games + Learning + Society Conference* (pp. 3–11). ETC Press.
- Amiel, T., & Reeves, T. C. (2008). Design-based research and educational technology: rethinking technology and the research agenda. *Educational Technology & Society*, 11(4), 29–40.
- Anderson, T., & Shattuck, J. (2012). Design-based research: a decade of progress in education research? *Educational Researcher*, 41(1), 16–25.
- Araujo, F., Shapouri, M., Pandey, S., Hamlen, K. (2015). *Experiences with honey-patching in active cyber security education*. In: 8th Workshop on Cybersecurity Experimentation and Test (CSET, 2015).
- Banks, N. (2015). *Teach children to hack ethically to save them from dark side*. SC Magazine for Security Professionals. Retrieved November 10, 2015, from <http://www.scmagazineuk.com/teach-children-to-hack-ethically-to-save-them-from-dark-side/article/416104/>.
- Barab, S. A., & Kirshner, D. E. (2001). Guest editors' introduction: rethinking methodology in the learning sciences. *Journal of the Learning Sciences*, 10(1&2), 5–15.
- Barab, S., Thomas, M., Dodge, T., Newell, M., & Squire, K. (2004). Critical design ethnography: designing for change. *Anthropology in Education*, 35(2), 254–268.
- Barab, S., Thomas, M., Dodge, T., Carteaux, R., & Tuzun, H. (2005). Making learning fun: Quest Atlantis, a game without guns. *Educational Technology Research and Development*, 53, 86–107.
- Branch, R. M., & Merrill, M. D. (2012). Characteristics of instructional design models. In R. A. Reiser & J. V. Dempsey (Eds.), *Trends and issues in instructional design and technology* (3rd ed., pp. 8–16). Boston, MA: Pearson.
- Brown, A. L. (1992). Design experiments: theoretical and methodological challenges in creating complex interventions in classroom settings. *Journal of the Learning Sciences*, 2(2), 141–178.
- Brown, A., & Campione, J. (1996). Psychological theory and the design of innovative learning environments: on procedures, principles, and systems. In L. Schauble & R. Glaser (Eds.), *Innovations in learning: new environments for education* (pp. 289–325). Mahwah, NJ: Lawrence Erlbaum Associates.

- Brown, J. S., Collins, A., & Duguid, P. (1989). Situated cognition and the culture of learning. *Educational Researcher*, 18(1), 32–42.
- Bureau of Labor Statistics, U.S. Department of Labor. (2014) Information security analysts occupational outlook handbook, 2014–15 edition. Retrieved November, 12, 2015, from <http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm>.
- Center for Infrastructure Assurance and Security (CIAS) (2018). Cyber threat defender/Retrieved September 13, 2018 from <http://cias.utsa.edu/ctd.php>.
- Cobb, P., Confrey, J., diSessa, A., Lehrer, R., & Schauble, L. (2003). Design experiments in educational research. *Educational Researcher*, 32(1), 9–13.
- Collins, A. (1992). Towards a design science of education. In E. Scanlon & T. O'Shea (Eds.), *New directions in educational technology* (pp. 15–22). Berlin: Springer.
- Collins, A. (1999). The changing infrastructure of education research. In E. Lagemann & L. Shulman (Eds.), *Issues in education research* (pp. 289–298). San Francisco: Jossey-Bass.
- Collins, A., Joseph, D., & Bielaczyc, K. (2004). Design research: theoretical and methodological issues. *Journal of the Learning Sciences*, 13(1), 15–42.
- Design-Based Research Collective. (2003). Design based research: an emerging paradigm for educational inquiry. *Educational Researcher*, 32(1), 5–8.
- Gee, J. (2003). *What video games have to teach us about learning and literacy*. New York: Palgrave Macmillian.
- Glaser, B. (1978). *Theoretical sensitivity: advances in the methodology of grounded theory*. Mill Valley, CA: Sociology Press.
- Glaser, B. (1992). *Basics of grounded theory analysis: emergence vs. forcing*. Mill Valley, CA: Sociology Press.
- Glaser, B. (1998). *Doing grounded theory: issues and discussions*. Mill Valley, CA: Sociology Press.
- Glaser, B., & Strauss, A. (1967). *The discovery of grounded theory: strategies for qualitative research*. Chicago: Aldine.
- Hasbro (2016). *Hasbro: annual report 2016*. Retrieved July 27, 2017 from, http://files.shareholder.com/downloads/HAS/4884637548x0x935515/842829F9-4911-4850-8770-B8106CFAA447/Hasbro_2016_Annual_Report_Final.pdf.
- Hoadley, C. (2002). Creating context: design-based research in creating and understanding CSCL. In G. Stahl (Ed.), *Computer support for collaborative learning 2002* (pp. 453–462). Mahwah, NJ: Lawrence Erlbaum Associates.
- Ito, M. (2005). Technologies of the childhood imagination: Yugioh, media mixes, and everyday cultural production. In J. Karaganis & N. Jeremijenko (Eds.), *Structures of participation in digital culture* (pp. 88–110). Durham, NC: Duke University Press.
- Lave, J., & Wenger, E. (1991). *Situated learning: legitimate peripheral participation*. Cambridge: Cambridge University Press.
- Marczewski, A. (2013). Gamification: a simple introduction. E-Book p. 3. ISBN 978-1-4717-9866-5.
- McKenney, S., & Reeves, T. C. (2014). Educational design research. In J. M. Spector, M. D. Merrill, J. Elen, & M. J. Bishop (Eds.), *Handbook of research on educational communications and technology* (4th ed., pp. 131–140). New York: Springer.
- McKenney, S., & Reeves, T. C. (2018). *Conducting educational design research*. New York, NY: Routledge.
- National Initiative for Cybersecurity Careers and Study. (2015). *Cybersecurity workforce planning*. Retrieved November 13, 2015, from <https://niccs.us-cert.gov/careers/workforce-planning>.
- Newman, D. (1990). Opportunities for research on the organizational impact of school computers. *Educational Researcher*, 19(3), 8–13.
- Obama, B. (2014). Statement by the president on the cybersecurity framework (press release). The White House Office of the Press Secretary. Retrieved November 13, 2015, from <http://www.whitehouse.gov/the-press-office/2014/02/12/statement-president-cybersecurity-framework>.
- Obama, B. (2015). Remarks by the president in state of the union address January 20, 2015. *The White House Office of the Press Secretary*. Retrieved November 12, 2015, from <https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015>.
- Pelling, N. (2011). The (short) prehistory of gamification. Retrieved December 5, 2018, from <http://nanodome.wordpress.com/2011/08/09/the-short-prehistory-of-gamification/>.
- Ponemon Institute (2017). The cost of cyber crime: insights on the security investments that make a difference. Publishd by Ponemon Institute and Accenture. Retrieved February 9, 2019 from: https://www.accenture.com/t20171006T095146Z__w_/us-en/_acnmedia/PDF-62/Accenture-2017CostCybercrime-US-FINAL.pdf#zoom=50.
- Reigeluth, C. M., & Frick, T. W. (1999). Formative research: a methodology for creating and improving design theories. In C. M. Reigeluth (Ed.), *Instructional-design theories and models* (Vol. II, pp. 633–651). Mahwah, NJ: Lawrence Erlbaum.
- Reinking, D., & Bradley, B. A. (2008). *On formative and design experiments: approaches to language and literacy research: an NCRL volume*. New York, NY: Teachers College Press.
- Squire, K. D. (2006). From content to context: videogames as designed experiences. *Educational Researcher*, 35(8), 19–29.
- Squire, K. D. (2011). *Video games and learning: teaching and participatory culture in the digital age*. New York, NY: Teachers College Press.
- Trump, D. J. (2017). Presidential executive order on strengthening the cybersecurity of federal networks and critical infrastructure. Retrieved June 1, 2018, from <https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/>.
- Turkay, S., Adinolf, S., & Tirthali, D. (2012). Collectible card games as learning tools. *Procedia- Social and Behavioral Sciences*, 46, 3701–3705.
- United States Department of Homeland Security (2011). Blueprint for a secure cyber future—the cybersecurity strategy for the homeland security enterprise. Retrieved November, 10 21015, from <http://www.dhs.gov/blueprint-secure-cyber-future>.
- United States Executive Office of the President. (2011). *Trustworthy cyberspace: strategic plan for the Federal Cybersecurity Research and Development Program*. Retrieved November 13, 2015, from www.whitehouse.gov/sites/default/files/microsites/ostp/fed_cybersecurity_rd_strategic_plan_2011.pdf.
- Wikipedia. (2017). List of the highest-grossing media franchises. (n.d.). In *Wikipedia*. Retrieved August 5, 2017, from https://en.wikipedia.org/wiki/List_of_the_highest-grossing_media_franchises.
- Wilshusen, G. C. (2015). *Cybersecurity: recent data breaches illustrate need for strong controls across federal agencies*. GAO Highlights. Retrieved November 12, 2015, from <https://www.gao.gov/assets/680/670935.pdf>.