Exploring the gamification of cybersecurity education in higher education institutions: An analytical study

Hanyu Xiao [1], *Hao* Wei [1], *Qichen* Liao [2], *Qiongwei* Ye [1,*] *Changlin* Cao [3], and *Yawen* Zhong [3]

[1]Yunnan University of Finance and Economics, Kunming, China
[2]Beijing Foreign Studies University, Beijing, China
[3]Guangzhou Institute for Industrial Development in Greater Bay Area, Guangzhou, China

Keywords: Higher education institutions, Cybersecurity education, Cyberattacks, Gamification.

Abstract. Our world has become increasingly dependent on electronic technology. As most economic, cultural, and social activities are conducted in cyberspace, how to protect data from cyberattacks has arisen as a prominent challenge. Cybersecurity education and training that improves awareness among personnel is recognized as an effective approach. Higher education institutions (HEIs) have become prime cyberattack targets as they hold vast amounts of valuable research and personal data. This paper analyses the state of cybersecurity in HEIs and the problems of cybersecurity education, and proposes the solution of gamification of cybersecurity education. A detailed feasibility analysis and recommendations for developing cybersecurity education games are provided. This paper expands the theories of gamified cybersecurity education in China, and sheds light on enhancing the effectiveness of cybersecurity education in HEIs through games.

1 Current state of cybersecurity in HEIs

Currently, individuals, businesses, organisations, and government agencies conduct most of their economic, cultural, and social activities and interactions in cyberspace. How to protect data from cyberattacks has arisen as a challenging issue. In recent years, China has encountered an exponential increase in cyberattacks, with malicious actors changing up their techniques and exploiting system vulnerabilities, misconfigurations, the Internet of Things (IoT), cloud computing and other emerging technologies [1]. On June 22nd, 2022, the Northwestern Polytechnical University in China reported cyberattacks from foreign attackers. The investigation report showed that phishing emails and multiple types of cyber weapons were used during the attacks, including jump servers, proxy servers and backdoors. These attacks have brought the issue of cybersecurity at key universities in China to the

* Corresponding author: yeqiongwei@163.com

fore. The rapidly changing cybersecurity landscape requires organization departments at all levels to keep pace with new threats to defend against cyberattacks [2].

On June 1st, 2017, the Cybersecurity Law of the People's Republic of China came into force. Following that, a series of laws and regulations were promulgated, which helped establish important systems for protection of critical information infrastructure security, network security, security assessment of cloud computing services, and data security management. Over 300 national standards for cybersecurity have been adopted [3], which play a guiding role in identifying and assessing the risks that cyberattacks pose to different organizations and assets.

One important aspect to consider when developing cybersecurity policies is to improve cybersecurity awareness of the personnel involved. No matter how much money an Internet organization pours into building firewalls, intrusion detection systems, or encryption, as long as the attackers have someone on the inside, those efforts will be of no avail. This prioritizes cyber education of staff in organizations that face cyber threats, as even simple understanding of cybersecurity and knowledge of how to make safe decisions can help avoid or at least mitigate cybersecurity risks [4]. An effective way to increase cybersecurity awareness is through education and training. Current training programs may have provided a good starting point for cybersecurity capacity building, but they are far from sufficient.

2 Cybersecurity challenges in HEIs in the new era

Because cybersecurity often involves the defence industry, up to now, most cybersecurity education programs have been led by national government units or agencies responsible for defence contract management [5]. In the information age when the risk of cyber conflict between nations is rapidly increasing, national infrastructures, businesses, and institutions have fallen victim to cyberattacks [6]. Cybersecurity threats are not limited to data theft and service disruption, but they also pose a menace to world peace – cyber war was included in the 60 cybersecurity predictions for 2019 [7].

Academic institutions are prime cyberattack targets as they hold vast amounts of valuable research and personal data which attract cybercriminals. HEIs are confronted with serious cybersecurity challenges, notably a shortage of expertise, funding and resources. The rapid technological change brings new cyber risks, which warrant new resolutions [8]. HEIs need to improve cybersecurity competencies of students and the faculty to defend against cyberattacks. Through a comprehensive analysis of the current state of cybersecurity in HEIs, the following challenges are identified.

2.1 Lack of innovation

First and foremost, despite being in the age of fast technological iteration, cybersecurity education in HEIs still follows superficial learning of cyberattacks through traditional teaching methods, such as lectures, seminars, and lab sessions. Current approaches to cybersecurity education have not utilized comprehensive theories, standards, or methods, and they fail to envision innovative strategies using underlying learning theories [9].

Secondly, the cybersecurity textbooks and learning materials used in HEIs still focus on how to respond to common risks. They are outdated, failing to address the real threats brought about by Internet technology developments and updates in the field of cybersecurity. Instead of adapting to the new cybersecurity ecology and environment, they are in effect more likely to cause mismatch between cybersecurity education and reality.

Thirdly, the content, mechanism and method are not innovative enough. To be specific, the content is not practical enough and cybersecurity training and practice are largely absent. As for the mechanism, HEIs fail to establish a management system suitable for

cybersecurity education in the mobile Internet era. As most HEIs don't have a special department for cybersecurity education and awareness, a unified organizing system is missing. Also, cybersecurity roles and responsibilities are not clearly defined and assigned [10]. Therefore, the practical cybersecurity education is in urgent need of a self-contained yet interesting teaching mechanism to encourage student engagement.

2.2 Lack of immersion

Firstly, HEIs appear to be unimaginative when it comes to cybersecurity education. The educational style is monotonous, emphasizing theory over practice. It puts students, the supposedly agents of their own learning, to a passive role, and fails to create a gamified learning environment to stimulate students' immersion. As a result, students lack the motivation to acquire knowledge of cybersecurity.

Secondly, studies have shown that games can be an effective tool not only for training but also for encouraging behaviour change [11]. With the development of virtual reality (VR) technology and digital games, immersion brings a virtual interactive environment that gives users a gaming experience. In contrast, there have been few encouraging developments of immersive learning experience in the education mode of HEIs, which impedes the effective and deep integration of educational games and classroom teaching.

Thirdly, college students are usually unaware of the importance of safeguarding national and university cybersecurity in the cyber world. They are used to the concept of knowledge acquisition, but not to the conscious participation in national and university cybersecurity practices. Therefore, there is an urgent need to propose innovative curricula and teaching methods in cybersecurity education. One of the rapidly growing areas in computer science education is "game-based learning". It encompasses VR games, network-based games, multi-user virtual environments, massively multiplayer online games, and simulations [12].

2.3 Lack of interaction

There is a lack of positive interaction mode in HEIs. In the educational mode of colleges and universities, educators are in the absolute, dominant position, and cybersecurity education follows a mechanical pattern of knowledge transfer that focuses solely on the teachers, without paying enough attention to the development needs of the students. The solidified identities of teachers and students further push the two groups apart, the most typical result being the lack of interaction among teachers, students, and between the two groups. When applied in cybersecurity education, this mode that lacks interaction will make students' learning stay only at the theoretical level, devoid of deep understanding or empathy for the cyber culture and cybersecurity education.

2.4 Lack of comprehensiveness

In general, the institution and mechanism of cybersecurity education in China's HEIs is gradually improving, and so is the overall cybersecurity awareness of students. However, given the exponential growth of cyberattacks, cybersecurity education in HEIs is not on track with the "prevention-oriented" principle and lacks comprehensive considerations. Although cybersecurity awareness has been included into the ideological and political education in HEIs, there are no full-time teachers to provide professional guidance to students. Meanwhile, the top-level design of cybersecurity education remains somewhat staid. There are no formal documents to guide the exploration of cybersecurity education games, which explains why HEIs are not willing to take the risk of innovating new approaches. In addition, HEIs are too dependent on teaching materials and overemphasize

knowledge of cybersecurity. This has led to deary indoctrination, in which gamification, a new teaching aid that is able to provide a new learning experience where interaction and entertainment are combined and effectiveness enhanced, is completely disregarded.

3 Feasibility analysis of applying gamification to cybersecurity education

Games as a new medium can complement and guide computer-based cybersecurity education and training. They provide an interesting and enjoyable educational environment where participants learn theories and concepts of cybersecurity and put them into practice. In particular, participants learn how to exploit the vulnerabilities in a dynamic environment and respond to attacks by developing defences and countermeasures on the spot. This way of learning enables participants to learn and master cybersecurity concepts at a more rapid rate [4]. In 2016, Awojana and Chow proposed incorporating a game-based learning system into the field of cybersecurity. This medium, they argued, would be attractive to young people, and help build a method for learning the basics of information security, and create a form of passion within the faculty and students, who could have some fun while receiving the training to become the next generation of cybersecurity professionals [13].

Similarly, courses that create gamification effects through simulation and imagination in teaching are common in HEIs. For example, the accounting courses at Yunnan University of Finance and Economics in Kunming, China have introduced business role-playing games and ERP sand table simulation business training. The game has incorporated practical business knowledge throughout the mechanics and is very well received among students [17]. In the sand table game, players accumulate assets by simulating business and business-related life behaviours, and they are ranked at the end according to their final asset totals. The competition combines the knowledge from macro finance, economics and accounting, which makes learning comprehensive and interesting. From the game developer's perspective, cybersecurity education allows participants to compete by following a set of rules and making vague and intrinsically meaningful choices [18]. For example, different sectors can choose different defence strategies when facing cyberattacks, similarly, different attackers with different targets can choose different attacking strategies.

3.1 Game frameworks applicable to cybersecurity education innovation

Usually, the game analysis frameworks use the elemental tetrad that splits games into four elements – mechanics, aesthetics, story, and technology — all of which can be closely integrated with cybersecurity education [14]. The basic stakeholders of cybersecurity activities, namely the attacker and the defender, are binary opposites, between which a simple, goal-oriented competition or confrontation relationship can be established. The stakeholders can be multiple opposing parties with both offensive and defensive functions who carry out offensive and defensive exercises, which can be a microcosm of the current global cybersecurity outlook. More broadly, the stakeholders can involve participants from different sectors in a certain cybersecurity environment, their positions corresponding to different cybersecurity events, such that attacking and defending simulations can be conducted in that very cybersecurity environment.

Cybersecurity education creates an environment where the educators output content to one or more persons. It is suitable for the framework of multiplayer games such as board games, card games, turn-based board games, and etc. The difficulty and value settings can be adjusted according to the player's mastery of cybersecurity knowledge. It is also possible to create and design complex and difficult games featuring interaction and

confrontation specifically for teachers and students of certain majors. In the game, the player can either write code to attack the system in the role of a hacker, or troubleshoot system vulnerabilities and manage risks as a cybersecurity administrator. For players who just want to have a smattering of cybersecurity, the game can be adjusted to a less challenging level and focus more on simulation and demonstration of narrative content. More complex game frameworks are capable of exploring cultural, moral, and philosophical themes through the cultural context of cybersecurity related content.

3.2 Student (player)-centred education

From the game developers' point of view, games must bring something to the player. This belief is consistent with the educators' faith of bringing knowledge to their students. The concept of student player-centred education game has two objectives: to design interesting cybersecurity games and to educate. Besides entertainment, this type of game can give participants a sense of gaining knowledge and accomplishment. The attitude of students towards knowledge is similar to that of gamers: some are willing to follow the rules and devote effort to learning; others ignore the rules and try to get the best result quickly by cheating; still others, who are not interested in the results at all, ignore the rules altogether. Developers and educators find a common goal here: to give students/players a good mindset, and to respect, rather than take advantage of them.

Generation Z students are tech-savvy at a very young age, and they have become used to short, efficient, and eye-catching media. Educators who follow the same routine will not be able to stop students from voting with their feet. Applying gamification and introducing eye-catching methods, such as creating conflicts, confrontations, and competitions give participants the chance to test their knowledge level. The autonomy in setting attack and defence targets and role-playing in cybersecurity-related scenarios are new experiences for students. They can promote students to gain joy and intrinsic motivation from competitions or creative contents, and encourage them to pay attention to the topic of cybersecurity while playing their roles. In particular, experiential learning and understanding of knowledge, including the background information of the defending and attacking sides of cyberattacks and threats, can only be obtained by letting participants restart, time and time again, new rounds or processes with different roles in the game.

3.3 Providing an immersive and interactive space for educational practices

Multiplayer games are interactions between players and content within the limits of game mechanics. In the embedded content of cybersecurity and under the set goal of positive education, the simulation of knowledge is transformed into the motivation of the players. Through the narrative adaptation of cybersecurity-related cases, the players' emotions are evoked: the desire to win is elevated to cybersecurity awareness, and they begin to vicariously think about the process according to the game mechanics. The immersive interaction allows players to achieve the goals set by the mechanics with the help of certain emotional feedback. The combination of immersion and interaction can evoke the internal drive for learning, transforming case studies into case experiences. To create a cybersecurity game, certain art designs need to be considered, including visual elements such as symbols, icons, characters, scenes, props, etc., which help enhance the vividness of the narrative and give a basis for the players' imagination. Gamification creates a virtual environment that provides participants (players) with an experience filled with emotionally charged story and various interaction ways, which yields an immersive learning experience.

In terms of single-player games, the players can create characters, participate in cybersecurity events, continuously earn cybersecurity-related achievements in the process,

thereby understanding, learning, reinforcing, and applying the knowledge, and even developing new relevant strategies and discovering new vulnerabilities. After the game, educators can facilitate discussion among players by reviewing their attack or defence strategies, providing immediate feedback on the correctness and effectiveness of the strategies, thus facilitating the construction of cybersecurity-related knowledge.

3.4 Foreign research on cybersecurity education games

Over the past decade, countries around the world have been actively engaged in the research on gamification of local cybersecurity education content. In 2015, Gestwicki and Stumbaugh summarized over 20 educational games on cybersecurity, both digital and non-digital, across Europe and the U.S., and drew the conclusion that all the games had advantages and disadvantages – they either had too little professional knowledge or had too high skills thresholds – but pointed out that the drawbacks might as well be transformed into development opportunities for cybersecurity education games [15].

Microsoft was the first to release "Elevation of Privilege (EoP)" in 2014 [16], a card game that helped improve identification of threats using the STRIDE methodology, i.e., spoofing, tampering, repudiation, information disclosure, denial of service, and escalation of privilege [17]. Similar board games that focus on cybersecurity education are: "Play2Prepare" [18], "Cyber Security-Requirements Awareness Game"[19], "Decision & Disruption" [20], and etc. Games that are targeted at cybersecurity education in schools include: "[d0x3d!]", a board game that aims to teach cybersecurity basics to K-12 students who have no access to a computer science curriculum or STEM education [21]; "The Security Cards", a card game that supports different types of educational activities in academic environments [22].

Although there have been many cases of gamification of cybersecurity education abroad for our reference, most of them are not suitable for China's realities, ideologies, and values, and therefore lessons cannot be directly borrowed. For example, Haggman set the UK and Russia as mutually hostile countries between which cyber warfare happens [23]. Such a hostile ideology that creates an "imaginary enemy" runs counter to the purpose of education and is not in line with the value of "a global community of shared future".

4 Recommendations for developing cybersecurity education games suitable for HEIs in China

4.1 Prioritizing education-oriented game mechanics

It is proved that incorporating games into learning will improve learning outcomes, and the effect is most prominent in multiplayer games [24]. However, due to the negative impact of gaming addiction, the promotion of gamification has been highly controversial in China. As games for pedagogical use, their mechanics should be designed in such a way that they are more like "tools". The class hours of the course should be considered when deciding the settlement period of the game results. It is recommended that all rounds or tasks be completed within 2 class hours and that the route of serious games be followed. The ideological orientation should be properly guided to prevent excessive stimulation and to prevent the transformation of cybersecurity education of students into training of malicious actors. To better manage the class, the teachers may start with board game and card game, and expand to single-player game or online multi-player game.

4.2 Keeping up with the times and follow China's cybersecurity standards

Introducing national cybersecurity standards is an important way to achieve the educational goals of cybersecurity education games. Game scenarios should be designed to facilitate, simulate and recreate complex events in real life. This coincides with the suggestion of Awojana and Chow: "Also, an improvement on the existing game based learning system is recommended to include the added features on awareness, defensive and attacker strategies. For future research, we would recommend an introduction of naturality to further improve on the existing features on the Multiplayer Game category for maximum effectiveness" [24]. Therefore, the preferrable approach to enhance the authenticity of cybersecurity education games is to combine regulations and moral ethics in the real world [24].

In 2020, the National Information Security Standardization Technical Committee of China released 26 national standards, which provided whole-field regulation of and guide to information security. The provisions are highly valuable and can be used as direct references for games to set values, devise mechanics, and design cultural backgrounds. Only by incorporating the national cybersecurity standards, can the games initiate a dimensional collapse strike against the one-sided negative opinions on games, establish the meaning of games as teaching tools, and achieve the goal of entertaining for learning and learning for practice.

4.3 Assembling a comprehensive talent team for effective management

The content and form of gamification vary depending on the target audience of cybersecurity education. Therefore, a game design cannot be regarded as the one-size-fits-all solution to different educational situations. Gamified cybersecurity design should adhere to the five principles of environment dependence, target values, characteristic differences, scientific tasks, and group dynamics, set different environments and goals, combine different game elements, and transform complex tasks into comprehensible and engaging narrative content. The members of the game development team, as needed, should be from various disciplines, including cybersecurity, gamification design, pedagogy, psychology, graphic design, screenwriting, law, game programming, etc. Mechanics, play rules and narratives should be designed according to the target students' knowledge of cybersecurity and the level of learning they are required to achieve to promote effective learning. Since a game needs to go through numerous rounds of modifications and tests, a certain amount of research on the game process and participants' feedback is also warranted to facilitate the improvement of the game and enrich the theory of gamification education in China.

4.4 Incorporating cultural settings with Chinese characteristics to enhance influence

Drawing lessons from the existing cybersecurity education games made by foreign firms is beneficial to conducting independent research and production of gamified cybersecurity education tools in China. However, as different games are created on country-specific contexts, ideologies and social systems, we should avoid direct copying and plagiarism when learning from them. Our ultimate goal is to create cybersecurity education games suitable for Chinese college students. It naturally follows that stricter criteria and standards are set in terms of the original quality of game content and mechanics. The setting of the games should be embedded with culture featuring excellent Chinese characteristics, tell China's story, innovate Chinese game mechanics and technology, and pay more attention to improving the discourse system of Chinese culture. For example, organizations such as the Red Hackers' Alliance, Internet Security Base, and China Eagle Union have fought against

hegemony by “hacking”, protecting national security, upholding justice, and forming the Chinese “hacking culture”. These are positive and high-quality themes for the design of cybersecurity education games, and are the support for strengthening the players’ sense of justice and evoking the feeling of patriotism.

This work was supported by the Prominent Educator Program: Yunnan [2018]11, Kunming E-Business and Internet Finance R&D Center (KEIRDC[2020]).

References

1. Y. Li and Q. Liu, Energy Reports **7**, 8176-8186 (2021)
2. https://baijiahao.baidu.com/s?id=1743132415536145988&wfr=spider&for=pc (2022)
3. Editorial Board, China Cyberspace, **6** (2022)
4. E. Trickel, F. Disperati, E. Gustafso, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupé, G. Vigna, *2017 USENIX Workshop on Advances in Security Education (ASE 17)* (2017)
5. G. C. Kessler and J. Ramsay, Journal of Homeland Security Education, **2**, 35 (2013)
6. E. Johnson and N. Willey, IEEE Security and Privacy, **9**, 18-25 (2011)
7. Y. Kolli and A. Y. Javaid, *Proceedings of the International Conference on Frontiers in Education: Computer Science and Computer Engineering (FECS)* 23-29 (2019)
8. D. Miles, *2011Second Worldwide Cybersecurity Summit (WCS)* 1-3 (2011)
9. B. Martini and K. K. R. Choo, *Proceedings of Twenty Second European Conference on Information Systems* (2014).
10. Q. Liu, Y. He and S. H. Yang, Journal of Chongqing University (Social Science Edition), **5**, 218-226 (2018)
11. M. Salazar, J.Gaviria, C. Laorden, et al., *2013 IEEE Global Engineering Education Conference (EDUCON)* 602-607 (2013)
12. A. Kumar, S. Gupta, A. Rai and S. Sinha, International Journal of Scientific and Research Publications, **3**, 1-5 (2013)
13. J. L. Qin and H. L. Leng, Journal of Guangxi College of Education, **2**, 144-151 (2022)
14. J. G. Bond, *Introduction to Game Design, Prototyping, and Development* (Addison-Wesley Professional, 2017)
15. P. Gestwicki and K. Stumbaugh, *2015 Computer Games: AI, Animation, Mobile, Multimedia, Educational and Serious Games (CGAMES)* 131-137 (2015)
16. A. Shostack, *Summit on Gaming, Games, and Gamification in Security Education* (2014)
17. B. Potter, Network Security, **1**, 15–18 (2009)
18. I. Graffer, M. Bartnes and K. Bernsmed, Norsk Informasjonssikkerhetskonferanse (NISK), 58-69 (2015)
19. A. Yasin, L. Liu, T. Li, R. Fatima, J. Wang, IET Software, **13**,159–169 (2019)
20. S. Frey, A. Rashid, P. Anthonysamy, M. Pinto-Albuquerque, S.A. Naqvi, IEEE Trans. Software Eng, **45**, 521–536 (2019)
21. M. Gondree, Z.N. Peterson, *CSET* (2013)
22. http://securitycards.cs.washington.edu/

23. A. Haggman, *Cyber wargaming: Finding, designing, and playing wargames for cyber security education* (2019).
24. T. Awojana and T. S. Chou, *2019 Conference for Industry and Education Collaboration. American Society for Engineering Education* (2019)