A review of taxonomies of cybersecurity educational games*

Nipuna Hiranya Weeratunge[0000−0003−4612−0342] and Rune Hjelsvold[0000−0002−5955−1603]

Norwegian University of Science and Technology
{nipuna.h.weeratunge,rune.hjelsvold}@ntnu.no

Abstract. Presently, cybersecurity awareness is an essential skill expected from all audiences that range from small children to older adults. Moreover, serious games and gamification has been used in cybersecurity education for years with interesting results. Currently, there exists a multitude of cybersecurity games that target different cybersecurity skills and topics using a wide range of game genres and approaches. With the existence of such a variety of games, a classification taxonomy is of the utmost importance. A proper classification taxonomy can allow researchers to gauge the existing cybersecurity games as well as to place their proposed cybersecurity games in the pantheon of existing games. Thus, this research work conducted a literature review aimed from 2018 to August, 2023 to examine the existing taxonomies for cybersecurity educational games. It was observed that there exists several taxonomies for cybersecurity games but comprehensive taxonomies, especially aimed at cybersecurity serious games are lacking. Moreover, the review also identified some potential taxonomy candidates that are used in education games in general but are yet to be used in the scope of cybersecurity. Lastly, the review suggests an extended and unified cybersecurity educational game taxonomy by merging some of the available educational game taxonomies.

Keywords: literature review · cybersecurity · computer science education · educational games · gamification

1 Introduction

In today's fast paced world, cybersecurity is of the utmost importance where repercussions can occur across multiple industries and use cases. Moreover, according to the Statista's Cybersecurity Outlook, it is expected that the global cost of cybercrimes will surge in the next five years, increasing from $8.44 trillion in 2022 to $23.84 trillion by 2027 [15]. Hence, a good knowledge on cybersecurity is a vital skill expected from everyone, such as students, industry professionals, general public, etc. However, the World Economic Forum estimates that globally there is about a 3.12 million gap in the cybersecurity workforce with a more

* Supported by Excited – the Center for Excellent IT Education

than 2 million gap in the Asia-Pacific region alone [27]. Thus, many governments and countries have implemented public initiatives, such as the *National Cyber Security Awareness Month* to increase the cybersecurity knowledge and proper cybersecurity practices of their citizens [3] [2] [4].

Gamification is the use of game based features and mechanics, such as leaderboards, points and badges in non-game contexts, with the aim of encouraging participant engagement and motivation [17]. Similarly, games that have been designated for a different purpose other than entertainment are classified as serious games [24]. It has been reported that serious games and gamification have been utilized in education for a substantial time with many positive results [17] [24]. The games and gamification features employed in education tend to have distinctive features and classifications. Hence, the primary goal of this literature review survey is to explore the existing taxonomies of educational games for cybersecurity, with respect to, game related concepts, such as game genre, gamification elements and game motivators as well as educational concepts, such as pedagogical approach, knowledge type and target audience. This study can be beneficial for multiple target audiences that includes, researchers, practitioners/ educators and game developers where researchers can employ this study when analysing existing games and classifications while practitioners/educators can find existing educational games for use, according to their needs and specifications. For instance, the authors of [18] present a rather rudimentary classification of serious games in cybersecurity based on the topics they cover and the game purpose. Hence, it is our belief that a more general, flexible and comprehensive taxonomy could be beneficial for such researchers when analysing existing cybersecurity educational games. Moreover, game developers can use this study as an aid in scoping their educational game development project, in terms of target audience, proficiency level and topic of focus.

2 Related Work

This section will explore the existing literature on taxonomies on cybersecurity educational games. The authors of [5] present a newly developed taxonomy of the most common cybersecurity training methods with a comparison among them along various factors. The taxonomy consists of the 3 main types of delivery types, namely face-to-face class, self-directed class, and embedded class. The face-to-face class contains delivery methods, such as lecture-based, workshop based and story-based while examples for self-directed delivery methods include web-based training, text-based, video-based, and game-based approaches.

In addition, the authors of [30] present a grouping and classifications of cybersecurity research to propose an easily referenceable taxonomy of the cybersecurity research topics. In order to introduce this taxonomy, the authors conducted a literature survey regarding various cybersecurity research during the past five years which yielded 99 studies that were in turn grouped based on the research topic similarities. The study categorized the cybersecurity research topics into 8 areas, (1) Applied cybersecurity, (2) Cybersecurity data science, (3) Cyber-

security education and training, (4) Cybersecurity incidents, (5) Cybersecurity management and policy, (6) Cybersecurity technology, (7) Human and social cybersecurity and (8) Theories in cybersecurity.

Lastly, the authors of [33] present a review that covers academic publications and industry products with respect to tools utilized in cybersecurity awareness and education aimed at non-expert end-users developed in the past 20 years. They further maintain that through the search, 119 tools were identified and classified into five broad categories, such as digital games, film and animation, tabletop games, learning modules and comics. Moreover, the authors report that online games and short animated films were the most prevalent media for cybersecurity education.

Hence, a review of existing literature suggested that most of the existing taxonomies mainly group cybersecurity education related topics with regards to the primary research topic or the delivery method/media. Therefore, there is a lack of a flexible and general taxonomy that can be applied to a wide variety of cybersecurity educational games and their respective applications.

3 Methodology

The research methodology utilized in this work is a literature review survey. The keywords **("educational games" OR "cybersecurity educational games") AND taxonomy** were run on databases, such as *IEEE Xplore, ACM Digital Library, SpringerLink* and *Google Scholar* digital libraries to search for studies. Moreover, snowballing technique was also used to generate more studies by following references in the selected studies. The search was limited to the last five years with the time window set to 2018 - August, 2023.

The research questions for this study are:

- RQ1: What are the existing taxonomies for cybersecurity educational games?
- RQ2: How may the existing taxonomies fit into an extended and unified taxonomy for cybersecurity educational game concepts?

4 Results

This section details the results from the literature review. Firstly, the existing taxonomies for cybersecurity educational games will be presented.

4.1 Existing taxonomies for cybersecurity educational games

Academic benchmarks and industry standards in cybersecurity can be beneficial for a cybersecurity educational games taxonomy since these would already have categories and classifications that can aid the taxonomy. Hence, the authors of [11] present a novel, multi-faceted approach for analyzing popular open-source cybersecurity educational games with respect of their alignment with the standard academic and industry benchmarks. The primary characteristics of each of the benchmark and standard taxonomy is as follows,

- CSEC2017 curricular guidelines [9]
  Description: Mainly deals with *Knowledge Areas* and *Knowledge Units* covered by each game. For instance, Knowledge Areas can be *Data Security* and *System Security* while the Knowledge Units investigate at a more granular level with topics, such as *Social Engineering* and *Authentication*.
- National Initiative for Cybersecurity Education (NICE) [26]
  Description: Mainly deals with workforce functions covered in each game, as well as the specialty areas and work roles within each workforce function. For instance, the workforce function could be *Oversee and Govern* with the speciality area being *Training Education and Awareness* and the work role is *Cyber Instructor*.
- Cybersecurity Assessment Tools (CATS) model [28]
  Description: Mainly maps each game to *Cybersecurity Concept Inventory (CCI)* and *Cybersecurity Curriculum Assessment (CCA)* topics. For instance, *CCI* could be *Identify a vulnerability* with the *CCA* being *Authentication*.
- National Security Agency (NSA) GenCyber concepts [16]
  Description: Mainly maps each game to *GenCyber SecurityFirst Concepts*, such as *Integrity* and *Think Like an Adversary*.

The authors of [22] propose a flexible taxonomy for Interactive Cyber Training and Education (ICTE) with a detailed description of all components with a focus on technical realization that covers all phases of the exercise life cycle. The taxonomy details the technical setup, audience, training environment and the training setup for each game and is depicted in Figure 1b. Moreover, since this taxonomy provides a broad and detailed classification, it could be used as a base taxonomy for the classification of cybersecurity educational games.

4.2 Potential taxonomies for cybersecurity educational games

Even though the previously presented cybersecurity related taxonomies discuss the alignment with standards and benchmarks as well as ICTE implementation components, there are important factors that are missing. For instance, the employed pedagogical approach, addressed knowledge type, utilized gamification factors and game motivators can add value to an educational game taxonomy.

The authors of [20] lists the type of pedagogical foundations inherent in math games, using Kebritchi and Hirumi's (2008) framework [21]. The list of pedagogical foundations for math based games are Direct *Instruction/Drill & Practice, Experiential Learning, Discovery Learning, Situated cognition* and *Constructivist Learning*. These pedagogical approaches mainly describe which learning method and the key principles employed by the game. For instance, in the pedagogical approach *Experiential Learning* learning and teaching in games happen by doing and solving real-life problems through experiencing and interacting with the environment.

Similarly, the authors of [23] provide a revision to the taxonomy provided by Benjamin S. Bloom [1]. Furthermore, the Knowledge domain in the revised Bloom's taxonomy includes the following categories, *Factual Knowledge, Conceptual Knowledge, Procedural Knowledge* and *Metacognitive Knowledge*. These categories essentially describe the knowledge type gained by the learner. For example, *Procedural Knowledge* based educational methods describe how to do something with methods of inquiry, and criteria for using skills, algorithms, techniques.

The addition of game motivators and game design principles to a educational games taxonomy can be beneficial for many audiences, especially for game developers as it can allow them to position their games properly. Hence, the authors of [25] have conducted a literature review to create a comprehensive taxonomy of 56 game motivators in 14 classes as well as a taxonomy of 54 educational game design principles in 13 classes. The game motivators include aspects such as, challenge (e.g. a task that is suitable for for the player's skill level), competition (e.g. compete with other players to reach a goal) and many more. Educational game designers can utilize these motivators as a starting point for designing new game-based interventions, in addition to evaluating existing games. Similarly, the taxonomy of game design principles focus on categories, such as feedback (e.g. instructions & tutorials and immediate & useful feedback), social play (e.g. means for social communication & interaction and opportunities for collaboration & competition) and many more.

Investigating how the educational content is delivered in interactive educational games can add a valuable dimension to a educational games taxonomy. Thus, the authors of [10] present a taxonomy analyzing design elements that fostered learning and delivered educational content for interactive visual novels, which are a sub-genre of interactive narratives that consist of interactive experiences where players can create or impact a storyline through certain actions. The main categories of the taxonomy is given below,

- Teaching Through Choice

  Description: The focus on learning and story progression is through the selection of explicit choices for the player's character.
- Teaching Through Scripted Sequences

  Description: The player's progression through the story are reliant upon scripted sequences (i.e., scenarios) and requires the player to conduct the designer's exact intended actions before allowing them to progress.
- Teaching Through Mini-games

  Description: In this strategy, players are taught concepts through playing mini-games which have been used effectively in educational games.
- Teaching Through Exploration

  Description: The player is taught concepts through exploration of the game's world where the teaching relies on self exploration, and often times employs a hidden story structure where players have to discover story content in order to progress.

– Non-interactive Teaching

  Description: In this strategy, teaching relies solely on narration and character dialogue where players are taught passively with learners receiving information without doing any activities to learn new concepts or reinforce existing ones.

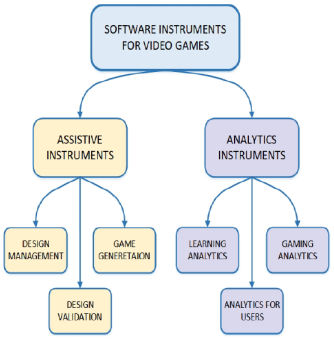
Evaluating the learning, user and gaming analytics can add more credibility to a educational game. Hence, the authors of [12] propose a taxonomy named *Taxonomy of Instruments for Management and Evaluation of the Design of Video Games for Education (TIMED-VGE)* to aid the development of better educational video games with personalized and high-value learning content combined with the adaptive video gameplay process and improved user-experience. The category *Assistive Instruments* deals with the creation of an educational game through concepts, such as design management, design validation and game generation. Conversely, the category *Analytics Instruments* can provide insights from previously generated and evaluated games through methods such as, learning analytics, analytics for users and gaming analytics. This taxonomy is shown in Figure 1a.

In addition, the authors of [8] propose an extended taxonomy for categorising innovation and design educational games. This proposed taxonomy is rather comprehensive as it deals with elements of the game such as, the target audience, purpose of the game, utilized platform, etc. This taxonomy is shown in Figure 2. Lastly, the taxonomy also provides provisions for multiple selections within a category. For instance, a game could have multiple target audiences and multiple intended purposes. Similarly, the authors of [32] conducted a literature review on educational games and have classified the themes found in the studies into three main categories, cognition, emotion and social skills interactions. The cognition category mainly deals with the educational methods and aspects addressed by the games, such as experiences, motivation, pedagogy, reasoning, memory etc. while the emotion category includes psychological and emotional aspects of educational games, such as enjoyment, engagement, immersion etc. Finally, the social skills interaction category includes elements such as communication, interaction, behavior and attitude that players will experience while playing educational games.

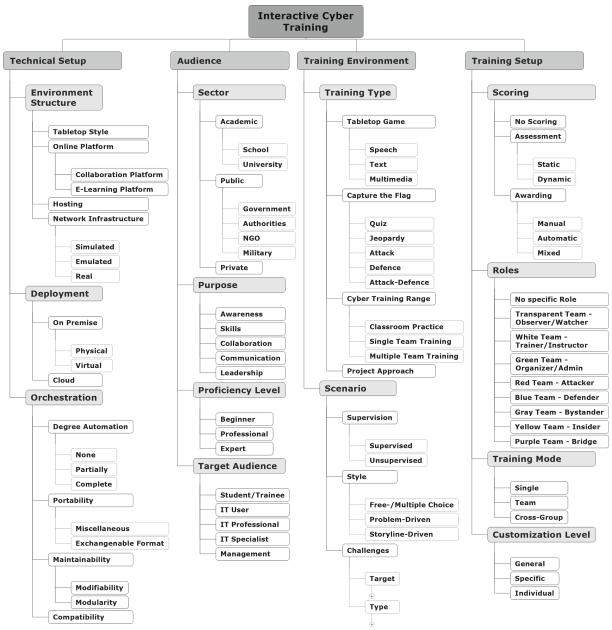
Conversely, analyzing the utilized gamification elements of an educational game would add value to an educational game taxonomy. Therefore, the authors of [14] have chosen to classify the gamification elements of educational games where the gamification elements are classified into two categories as given below,

– Tangible

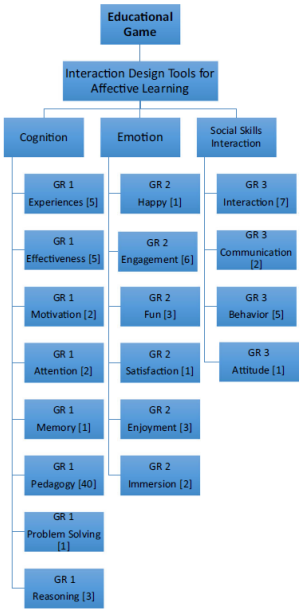
  Description: Describes any game element that can be embodied in an object and provide interaction between the user and the machine or the application. For instance *Competition* (e.g. statistics on the top performers at each level of the game) and *Convenience* (e.g. interaction with the game mostly through simple actions of clicks on buttons, swiping or typing few letters)



(a) Taxonomy of Instruments for Management and Evaluation of the Design of Video Games for Education[12]



(b) Taxonomy of interactive cyber training and education systems [22]



(c) Classification of guideline recommendations (GR) for game as effective learning tools [32]

Fig. 1: Taxonomies of games for education and training

– Intangible

Description: Describes any game element that cannot be embodied in an object that provides interaction between the user and the machine. For instance *Information Quality* (e.g. use current and modern vocabulary,

Game approach: ○ Gamification ○ Serious game ○ Simulation game
Type of platform does the game require: ○ Digital ○ Non-digital
Public/ targeted user: □ Children □ Students □ Professional
Placement of game: ○ During ○ After
Game purpose: □ Spread a message □ Educate □ Train
Involvement of participants: ○ Single player ○ Multi players
Innovation process stage: □ Design □ Realisation □ Service system-supply chain □ Business
Design stage: □ Task clarification □ Conceptual design □ Embodiment design □ Detail design
Design Thinking process stage: □ Data gathering about user needs □ Idea generation □ Testing
Evaluation level: □ Reaction □ Learning □ Behaviour □ Results

Fig. 2: Identified categories for classification (Legend: ○ Radio button, □ Checkbox)[8]

divided into few categories) and *Cooperation* (e.g. users can trade score for help and hints, through some social network)

Similarly, the authors of [31] have also chosen to classify gamification elements within the education domain and have proposed a taxonomy of 21 game elements as well as the affected player behavior. An few of the elements of the proposed taxonomy is given below,

- Acknowledgement
  Description: Refers to feedback that praises players' specific actions, such as badges, medals, trophies. Affected behavior: Engagement
- Economy
  Description: Transactions within the game, monetising game values and other elements, such as markets, transaction, exchange. Affected behavior: Engagement
- Cooperation
  Description: When two or more players collaborate to achieve a common goal, such as teamwork, co-op missions. Affected behavior: Motivation

These taxonomies have not been used to classify cybersecurity educational games but this review argues that they are indeed good candidates to be used for the classification of cybersecurity educational games.

4.3 Analysis of some cybersecurity educational games with the presented taxonomies

In this section a few cybersecurity educational games are classified according to some of the above presented taxonomies. Five cybersecurity educational games were chosen and were evaluated. This is depicted in Table 2.

5 Discussion

This section discusses the results from the previous section.

5.1 Characteristics of existing taxonomies of cybersecurity educational games

It is interesting to analyze the presented cybersecurity educational games taxonomies with respect to their 1) motivation 2) contribution 3) evaluation and 4) limitations. This is shown in Table 1.

Contributing Study	Motivation	Contribution	Evaluation	Limitations
[11]	A lack of taxonomies aligned with existing cybersecurity benchmarks in academic and industry standards	A taxonomy that is aligned with the CSEC2017 curricular guidelines, the Cybersecurity Assessment Tools (CATS) model, the National Security Agency (NSA) GenCyber concepts and the National Initiative for Cybersecurity Education (NICE)	Evaluated with 14 cybersecurity educational games	Mainly analyzes games with respect to benchmarks & standards and does not investigate elements, such as target audience, proficiency level, game genre, single/multi-player, objective of the game etc.
[22]	A lack of a general classification to aid the extension and implementation of ICTE	A flexible taxonomy for ICTE with a detailed description of all components with a focus on technical realization that covers all phases of the exercise life cycle	Evaluated by classifying a Capture-The-Flag (CTF) event	A flexible taxonomy but could be improved further to classify different genres of educational games

Table 1: Cybersecurity educational games taxonomies

5.2 An extended and unified taxonomy of cybersecurity educational games

By examining Table 1, it can be seen that there does not exist a single comprehensive taxonomy to properly classify cybersecurity educational games. Moreover by observing Table 2, it can be observed that general educational games taxonomies can act as potential candidates to classify cybersecurity educational games as well. Hence, this review suggests a unified taxonomy for cybersecurity educational games.

Thus, the ICTE taxonomy presented in [22] can be used as the base taxonomy since it provides a flexible and general representation of ICTE. Moreover, elements from the following taxonomies can be added to this base taxonomy,

- Standards and benchmarks from [11]
- Pedagogical approaches from [20] and educational content delivery from [10]
- Knowledge in cognitive domain from [23]
- Game motivators from [25]
- Guideline recommendations from [32]
- Gamification elements from [14] and [31]
- Evaluation elements from [12]

Figure 3 denotes this suggested unified taxonomy in a more higher level representation and provides a general and flexible approach that could be utilized to classify most cybersecurity educational games. For instance, the taxonomy contains four main elements, namely the technical setup which details the technical aspects of the educational game, the audience aspect which explains the purpose, topics and proficiency levels, the game environment with the genre, knowledge type and pedagogical approaches and the game setup which details the number of players and evaluation setup. As mentioned earlier, the base of the taxonomy consists of the ICTE taxonomy presented in [22]. Key points of this taxonomy is given below,

- Standards and benchmarks from [11] was included under audience since these standards and benchmarks can categorize cybersecurity educational games in terms of the proficiency level, target audience and primary education topic.
- The pedagogical approaches from [20] and educational content delivery from [10] was included under game environment since it directly ties to the learning method employed by the game.
- Knowledge in cognitive domain from [23] was also included under game environment since it describes knowledge gained by the learner through the game.
- Game motivators from [25] was included under game environment since the development of the game environment depends on the different type of game motivators.
- Guideline recommendations from [32] was included under game environment since the factors of interaction design tools, such as cognition, emotion and social skills interaction can directly affect the utilized game environment.
- Gamification elements from [14] and [31] was listed under game environment since the employed gamification elements will have an impact of the game environment.
- Evaluation elements from [12] was listed under game setup since how the evaluation would be conducted will depend on how the game is setup.

Hence, by observing Figure 3, it can be postulated that the presented extended and unified taxonomy would carry the best traits from all of the presented taxonomies and thus, can be used to classify cybersecurity educational games effectively.

6 Conclusion

This survey conducted a literature review from 2018 to August, 2023 to examine the existing taxonomies for cybersecurity educational games. Moreover, existing cybersecurity educational game taxonomies were analyzed along with general educational game taxonomies that had yet to be applied for cybersecurity educational games. Even though a few general and broad taxonomies were discovered, the review notes that there is a lack of comprehensive taxonomies for cybersecurity educational games where the ICTE taxonomy presented in

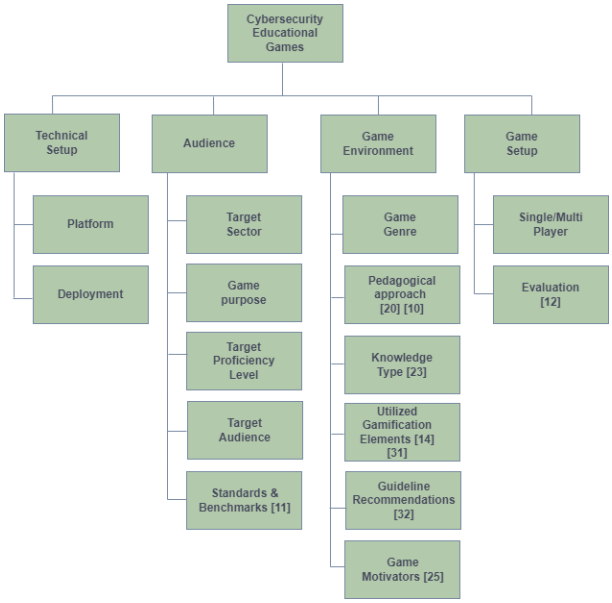


Fig. 3: Unified taxonomy for cybersecurity educational games

[22] providing the closest candidate to a general and comprehensive taxonomy. Hence, the review presents a unified and extended taxonomy that consists of merging existing educational games taxonomies to provide a general methodology to classify existing and new cybersecurity educational games. This presented taxonomy can investigate cybersecurity educational games, with respect to, technical setup, target audience, game environment and game setup. Moreover, such taxonomies can support cybersecurity education game development by outlining the different design choices.

One of the main limitations of this study is the absence of validation by relevant external stakeholders, such as cybersecurity researchers, teachers/educators and educational game developers. Moreover, the search for existing studies on taxonomies were limited to the databases *IEEE Xplore, ACM Digital Library, SpringerLink* and *Google Scholar*, to keep the review work more manageable. Lastly, this presented taxonomy has not been evaluated against existing cybersecurity educational games.

As future work, it is planned to add external validation for the presented taxonomy by conducting a joint evaluation with external stakeholders and against existing cybersecurity educational games. Finally, more studies will be included from other databases, such as *Web of Science, ScienceDirect* and *Wiley Online Library.*

Cybersecurity educational game	**Educational game taxonomies**							
	[11]	[22]	[20]	[23]	[25]	[10]	[8]	[32]
Social engineering and information security game [19]	SEC2017:Human Security-Social Engineering, NICE:Protect and Defend-Cyber Defense Analysis-Cyber Defense Analyst, CCI:Identify Risky Behaviors, CCA: Social engineering	Online platform, Academic-School, Awareness, Beginner, Student, Project Approach, Unsupervised, Story-line Driven, Blue Team-Defender, Single	Experiential Learning	Procedural Knowledge	Challenge, Feedback, Immersion, Real World Relation, Usefulness	Teaching Through Scripted Sequences	Serious game, Digital, Students, Educate, Single player, Testing	Experiences, Reasoning, Immersion, Enjoyment, Interaction
Laptop Security [29]	CSEC2017:Data Security-Data Integrity and Authentication, NICE:Protect and Defend-Cyber Defense Analysis-Cyber Defense Analyst, CCI:Identify vulnerabilities and failures, CCA: Analyze Threats	Online platform, Academic-School, Awareness, Beginner, Student, Multimedia, Unsupervised, Story-line Driven, Blue Team-Defender, Single	Experiential Learning	Procedural Knowledge	Challenge, Feedback, Immersion, Real World Relation, Usefulness	Teaching Through Scripted Sequences	Serious game, Digital, Students, Educate, Single player, Testing	Experiences, Reasoning, Immersion, Enjoyment, Interaction
CybAR [7]	CSEC2017:Connection Security-Distributed Systems Architecture, NICE: Analyze-Exploitation Analysis–ExploitationAnalyst, CCI:Identify vulnerabilities and failures, CCA: Analyze Threats	Online platform, Academic-University, Awareness, Beginner, Student, Multimedia, Unsupervised, Problem Driven, Blue Team-Defender, Single	Instruction/ Drill & Practice	Procedural Knowledge	Challenge, Feedback, Immersion, Real World Relation, Usefulness	Teaching Through Scripted Sequences	Serious game, Digital, Students, Spread a message & Educate, Single player, Testing	Memory, Reasoning, Immersion, Enjoyment
ARI 3D [13]	CSEC2017:Multiple-Multiple, NICE:Protect and Defend-Vulnerability Assessment and Management–Vulnerability Assessment Analyst, CCI:Devise a security plan, CCA: Assess vulnerabilities	Online platform, Academic-University, Awareness, Beginner, Student, Multimedia, Unsupervised, Story-line Driven, Blue Team-Defender, Single	Discovery Learning	Procedural Knowledge	Challenge, Feedback, Immersion, Fantasy, Usefulness	Teaching Through Exploration	Serious game, Digital, Students & Professionals, Educate, Single player, Testing	Experiences, Reasoning, Immersion, Enjoyment, Interaction
Happy Hippo [6]	CSEC2017:Connection Security-Cybercrime, NICE:Protect and Defend-Cyber Defense Analysis-Cyber Defense Analyst, CCI:Identify Risky Behaviors, CCA: Manage Risks	Online platform, Academic-School, Awareness, Beginner, Student, Multimedia, Supervised, Story-line Driven, Blue Team-Defender, Single	Instruction/ Drill & Practice	Procedural Knowledge	Challenge, Feedback, Immersion, Real World Relation, Usefulness	Teaching Through Mini-games	Serious game, Digital, Children, Train, Single player, Testing	Experiences, Reasoning, Immersion, Enjoyment, Interaction

Table 2: Cybersecurity educational games analyzed by taxonomies

References

1. Taxonomy of educational objectives: The classification of educational goals. Handbook 1: Cognitive domain (1956)
2. Cyber security awareness month (csam) (2021), https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2020/10/cyber-security-awareness-month.html
3. National cybersecurity awareness month (ncsam) (2021), https://www.cisa.gov/national-cyber-security-awareness-month
4. What is ecsm? (2021), https://cybersecuritymonth.eu/about-ecsm/
5. Alhashmi, A.A., Darem, A., Abawajy, J.: Taxonomy of cybersecurity awareness delivery methods: A countermeasure for phishing threats (2021)
6. Allers, J., Drevin, G.R., Snyman, D.P., Kruger, H.A., Drevin, L.: Children's awareness of digital wellness: a serious games approach. In: IFIP World Conference on Information Security Education. pp. 95–110. Springer (2021)
7. Alqahtani, H., Kavakli-Thorne, M.: Does decision-making style predict individuals' cybersecurity avoidance behaviour? In: HCI for Cybersecurity, Privacy and Trust: Second International Conference, HCI-CPT 2020, Held as Part of the 22nd HCI International Conference, HCII 2020, Copenhagen, Denmark, July 19–24, 2020, Proceedings 22. pp. 32–50. Springer (2020)
8. Bhatt, A.N., Acharya, S., Chakrabarti, A.: Extended taxonomy of design and innovation games to identify perspectives of development and evaluation. Proceedings of the Design Society **1**, 1547–1556 (2021)
9. Burley, D., Bishop, M., Buck, S., Ekstrom, J., Futcher, L., Gibson, D., Hawthorne, E., Kaza, S., Levy, Y., Parrish, A.: Cybersecurity curricula 2017: curriculum guidelines for post-secondary degree programs in cybersecurity. Joint Task Force on Cybersecurity Education (2017)
10. Camingue, J., Melcer, E.F., Carstensdottir, E.: A (visual) novel route to learning: a taxonomy of teaching strategies in visual novels. In: Proceedings of the 15th International Conference on the Foundations of Digital Games. pp. 1–13 (2020)
11. Chattopadhyay, A., Maschinot, C., Nestor, L.: Mirror mirror on the wall-what are cybersecurity educational games offering overall: A research study and gap analysis. In: 2021 IEEE Frontiers in Education Conference (FIE). pp. 1–8. IEEE (2021)
12. Dankov, Y., Bontchev, B.: Towards a taxonomy of instruments for facilitated design and evaluation of video games for education. In: Proceedings of the 21st International Conference on Computer Systems and Technologies. pp. 285–292 (2020)
13. DeCusatis, C., Gormanly, B., Alvarico, E., Dirahoui, O., McDonough, J., Sprague, B., Maloney, M., Avitable, D., Mah, B.: A cybersecurity awareness escape room using gamification design principles. In: 2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC). pp. 0765–0770. IEEE (2022)
14. Elaish, M.M., Hussein, M.H., Shuib, L., Ahmad, W.F.W., Becker, K.: A proposed gamification elements of educational games. In: 2021 International Conference on Computer & Information Sciences (ICCOINS). pp. 14–17. IEEE (2021)
15. Fleck, A.: Cybercrime expected to skyrocket in coming years (2022), https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/
16. GenCyber: Inspiring the next generation of cyber stars (2021), https://www.gen-cyber.com/
17. Hallifax, S., Serna, A., Marty, J.C., Lavoué, É.: Adaptive gamification in education: A literature review of current trends and developments. In: European Conference on Technology Enhanced Learning. pp. 294–307. Springer (2019)

18. Hill Jr, W.A., Fanuel, M., Yuan, X., Zhang, J., Sajad, S.: A survey of serious games for cybersecurity education and training (2020)
19. Jin, G., Tu, M., Kim, T.H., Heffron, J., White, J.: Game based cybersecurity training for high school students. In: Proceedings of the 49th ACM Technical Symposium on Computer Science Education. pp. 68–73 (2018)
20. Kacmaz, G., Dubé, A.K.: Examining pedagogical approaches and types of mathematics knowledge in educational games: A meta-analysis and critical review. Educational Research Review **35**, 100428 (2022). https://doi.org/https://doi.org/10.1016/j.edurev.2021.100428, https://www.sciencedirect.com/science/article/pii/S1747938X21000518
21. Kebritchi, M., et al.: Examining the pedagogical foundations of modern educational computer games. Computers & Education **51**(4), 1729–1743 (2008)
22. Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seeber, S., Pöhn, D., Hillmann, P.: Cyber taxi: A taxonomy of interactive cyber training and education systems. In: Model-driven Simulation and Training Environments for Cybersecurity: Second International Workshop, MSTEC 2020, Guildford, UK, September 14–18, 2020, Revised Selected Papers 2. pp. 3–21. Springer (2020)
23. Krathwohl, D.R.: A revision of bloom's taxonomy: An overview. Theory into practice **41**(4), 212–218 (2002)
24. Laamarti, F., Eid, M., El Saddik, A.: An overview of serious games. International Journal of Computer Games Technology **2014** (2014)
25. Laine, T.H., Lindberg, R.S.: Designing engaging games for education: A systematic literature review on game motivators and design principles. IEEE Transactions on Learning Technologies **13**(4), 804–821 (2020)
26. Newhouse, W., Keith, S., Scribner, B., Witte, G.: National initiative for cybersecurity education (nice) cybersecurity workforce framework. NIST special publication **800**(2017), 181 (2017)
27. Paul Mee, C.C.: Cybersecurity is too big a job for governments or business to handle alone (2021), https://www.weforum.org/agenda/2021/05/cybersecurity-governments-business/
28. Sherman, A.T., Oliva, L., DeLatte, D., Golaszewski, E., Neary, M., Patsourakos, K., Phatak, D., Scheponik, T., Herman, G.L., Thompson, J.: Creating a cybersecurity concept inventory: A status report on the cats project. arXiv preprint arXiv:1706.05092 (2017)
29. Sookhanaphibarn, K., Choensawat, W.: Educational games for cybersecurity awareness. In: 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE). pp. 424–428. IEEE (2020)
30. Suryotrisongko, H., Musashi, Y.: Review of cybersecurity research topics, taxonomy and challenges: Interdisciplinary perspective. In: 2019 IEEE 12th conference on service-oriented computing and applications (SOCA). pp. 162–167. IEEE (2019)
31. Toda, A.M., Oliveira, W., Klock, A.C., Palomino, P.T., Pimenta, M., Gasparini, I., Shi, L., Bittencourt, I., Isotani, S., Cristea, A.I.: A taxonomy of game elements for gamification in educational contexts: Proposal and evaluation. In: 2019 IEEE 19th international conference on advanced learning technologies (ICALT). vol. 2161, pp. 84–88. IEEE (2019)
32. Yusoff, Z., Kamsin, A., Shamshirband, S., Chronopoulos, A.T.: A survey of educational games as interaction design tools for affective learning: Thematic analysis taxonomy. Education and Information Technologies **23**, 393–418 (2018)
33. Zhang-Kennedy, L., Chiasson, S.: A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR) **54**(1), 1–39 (2021)