# Mirror Mirror On The Wall - What Are Cybersecurity Educational Games Offering Overall: A Research Study and Gap Analysis

Ankur Chattopadhyay
Computer Science Department
Northern Kentucky University
Highland Heights, Kentucky, USA
chattopada1@nku.edu

Chase Maschinot
Computer Science Department
Northern Kentucky University
Highland Heights, Kentucky, USA
maschinotc5@nku.edu

Laura Nestor
Computer Science Department
Northern Kentucky University
Highland Heights, Kentucky, USA
nestorl1@nku.edu

***Abstract* - Cybersecurity educational games are capable of meeting a variety of goals, including learning of fundamental cybersecurity concepts, exposure to cybersecurity literacy, basic awareness, experiential learning plus situational awareness, and being a medium for K-12 outreach, college level learning plus corporate training. Existing literature shows that there have been several prior research surveys focused on analyzing cybersecurity educational games from various viewpoints. However, to our knowledge, there has been no previous work that has analyzed cybersecurity educational games in terms of their alignment with the current benchmarks in academic and industry standards that include the cybersecurity curriculum plus assessment guidelines in higher education, the K-12 standardized cybersecurity concepts, and the cybersecurity job-related functions. In an effort to address this research gap, we use 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) framework for performing a unique analysis of a list of popular cybersecurity educational games, plus a few Capture the Flag (CTF) instances. The list of cyber educational games, which we study, comprises of Anti-Phishing Phil, Cyber Awareness Challenge, Cyber CIEGE, Cyber Protect, Nsteens, NOVA Labs, What.Hack, PASDJO, CyberStart Go, OnGuardOnline, Safe Online Surfing, and Interland. This non-traditional survey-based research work demonstrates a novel, multi-faceted approach for analyzing popular opensource cybersecurity educational games in terms of their alignment with the standard academic and industry benchmarks. Our survey results include conceptual mapping of these cyber educational games to (1) the CSEC2017 curricular knowledge areas (Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security and Societal Security), (2) the CATS concept inventory topics, including the Cybersecurity Concept Inventory (CCI), which pertains to basic first year college concepts, and the Cybersecurity Curriculum Assessment (CCA), which contains core concepts and learning outcomes for a college graduate, (3) the NSA GenCyber concepts (Defense in Depth, Confidentiality, Integrity, Availability, Think Like an Adversary and Keep It Simple), and (4) NICE framework-based specialized skill sets (Analyze, Collect & Operate, Investigate, Operate & Maintain, Oversee & Govern, Protect & Defend and Securely Provision). Our research provides a first-of its kind study and a user-friendly analysis of open-source cybersecurity educational games that can serve as an insightful reference for cybersecurity educators and other audiences for using these games. Additionally, in this full research paper, we exhibit how the results of our study can be used for performing an overall gap analysis with cybersecurity educational games in terms which benchmarks they cover and which they do not.**

## I. INTRODUCTION

As our world becomes increasingly digitalized and dependent on technology, cybersecurity risks and cybersecurity attacks have become a prevalent issue. This rise in cybercrime has revealed the importance of cybersecurity and the need for more education and awareness for not only cybersecurity professionals, but also the general public [7, 20, 22, 24, 26, 32, 33, 34, 36, 40]. In recent years, there have been a number of cybersecurity educational games developed for a variety of settings in order to address these concerns [3, 20, 21, 27, 28, 33, 37, 38]. These games have shown promising results in terms of their engagement and

pedagogical benefits, as well as being widely accessible and cost effective.

Previous research studies have conducted different surveys and analysis of cybersecurity educational games, including evaluation, performance assessment, and effectiveness in terms of learner engagement and motivation [3, 7, 20, 21, 22, 24, 26, 27, 28, 34]. There have been similar research surveys on the aspects of evaluation, performance assessment, and effectiveness of CTF s [4, 23, 29, 30, 35, 36, 39, 48], which have been surveyed separately from traditional cyber educational games. A recent survey on CTF s [48] has studied CTF challenges by mapping the solutions of the challenges to the IEEE/ACM curricular guidelines [1]. However, to our knowledge, no existing work has ever done an assessment study to see whether the traditional cybersecurity educational games meet the academic and industry recommendations, including desired outcomes from an educational perspective, like the ACM/IEEE recommendations [1], or other benchmarks.

A few prior studies on cybersecurity games [28, 41] have indicated future directions of work towards taxonomizing these games based upon learner assessment and needs from an educational perspective. The authors of [28] argue that since these cybersecurity games are traditionally considered as part of an informal learning space, it might not of much relevance to try developing a taxonomy for characterizing the role of a cybersecurity game in instruction, or its placement within formal educational curricula. With the extensive evolution of cybersecurity games, the academic community now have started to recognize the educational values of these games. The researchers in [41] propose a conceptual framework for taxonomizing cybersecurity learning and training elements, including games, that is driven by scenario execution flows (SEF) and standards for knowledge, skills and abilities (KSA), but no academic benchmarks or curricular assessment standards are utilized in this work.

In this paper, we address this research gap by proposing a unique conceptual analysis based taxonomy for cybersecurity educational games in terms of their alignments with the CSEC2017 guidelines [1], the NICE framework-based specialized skills [5], the CATS concept inventory topics [6], the NSA GenCyber concepts [2], and the corresponding learning outcomes respectively. To our knowledge, our approach is novel, and our survey results are the first of its kind, which lead to a unique way of analyzing cyber educational games from the standpoint of how well they meet academic and industry benchmarks.

## II. BACKGROUND

For our research study, a set of academic benchmarks and professional standards were carefully selected due to their popularity, recognition, wide scope of application (in both academia and industry) and user-specific relevance i.e., based upon the multiple user classes they are intended for. We implement a diverse, multi-layered taxonomy structure as part of our unique analysis in which we use these chosen frameworks and standards together to create a conceptual map out of a selected list of cybersecurity educational games.

The first academic benchmark, as used in our conceptual taxonomy, is CSEC2017 [1], which is a comprehensive curricular guide developed by the IEEE/ACM Joint Task Force on Cybersecurity (JTF) to provide a structure to the cybersecurity disciplinary curriculum in higher education. It is a reference framework for cybersecurity academic programs to meet the curricular needs of the discipline, while providing flexibility for a continually evolving field. The CSEC2017 is made up of 8 Knowledge Areas (KA s), which include Data Security, Software Security, Component Security, Connection Security, System Security, Human Security, Organizational Security, and Societal Security. Collectively, these KA s represent the full body of knowledge within the cybersecurity discipline. Each KA is broken into multiple Knowledge Units (KU s) that include more specific topics and essential concepts. CSEC2017 has been used in previous studies in cybersecurity education, involving conceptual taxonomy [25, 31, 42], but it has never been used in conjunction with classifying traditional cyber games.

The second academic benchmark, as used in this study, is the CATS assessment framework [6], which was developed to provide infrastructure for evidence-based improvement of cybersecurity education. We utilize the two CATS components - CCI and CCA, which originate from a Delphi process in which cybersecurity experts rated topics based on importance, difficulty, and timelessness to identify core cybersecurity concepts. The CCI includes 38 topics that should be mastered after a student's first course in the field and the CCA includes 53 topics that should be mastered by graduating students, who are about to enter the workforce. These have been used in prior cyber educational taxonomy studies [31], but never in the categorization of cyber games.

Our third chosen academic standard is the NSA GenCyber conceptual framework [2], which was developed to improve teaching and content for K-12 cybersecurity curricula, while increasing awareness, interest and learning opportunities among youth. These concepts, which are fundamental to understanding and practicing effective cybersecurity, include Defense in Depth, Confidentiality, Integrity, Availability, Think Like an Adversary, and Keep It Simple. Even though these GenCyber concepts have been in previous K-12 cybersecurity work [3, 34], they have not been used before in analysis of cyber games.

Our last and fourth selected benchmark for this study is the NICE workforce framework [5], which was developed as a fundamental reference resource for describing and sharing information about cybersecurity workforce knowledge requirements. The NICE framework consists of 7 Workforce Functions, which include Security Provision (SP), Operate and Maintain (OM), Oversee and Govern (OG), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO), and Investigate (IN). These workforce functions include Specialty Areas, which represent areas of more concentrated

work within each Workforce Function. Each Specialty Area is further divided into Work Roles, which describe a specific job or position as well as the knowledge, skills, and abilities (KSA s) and tasks included in the role. The NICE Framework has been used in prior taxonomy studies within cybersecurity education [25, 31, 33, 41], but there are no published taxonomy surveys of cyber games with it as the basis.

## III. METHODOLOGY

Our research began with a survey of existing literature focused on the current state of art cybersecurity educational games, were opensource, easily & freely accessible, and intended for a variety of audiences. We included the following list of such games in our study: Anti-Phishing Phil [8], Cyber Awareness Challenge [9], CyberCIEGE [10], CyberProtect [11], NSteens [12], NOVA Labs [13], What.Hack [14], PASDJO [15], CyberStart Go [16], OnGuardOnline [17], Safe Online Surfing [18], Interland [19], Targeted Attack: The Game [43], The Missing Link: A Cybersecurity Mystery [44], Aggie LIFE [45] and Education Arcade [46]. We also included a few CTF games in our study, such as, Facebook CTF (FBCTF), DEFCON, Mozilla, RuCTFe, PicoCTF and Bandit Overthewire [4, 23, 29]. It is to be noted that CTF s or live cybersecurity competitions were not the focus area of this study, as we were primarily interested in creating a taxonomy framework for describing the educational benchmark aligned contents in cyber games. Hence, we only surveyed a few CTF as part of this work.

In order to perform our unique analysis of the games, we played each game, observed its offered insights, gains & learnings, and noted the key cybersecurity concepts it taught. We then reviewed those conceptual takeaways and mapped them to the chosen academic & industry benchmarks accordingly. The conceptual mapping process we utilized for our unique taxonomy building is similar to prior research studies that are based upon conceptual analysis in cybersecurity education [25, 28, 31, 33, 41, 42]. To illustrate this process for better understanding, we provide a brief description of how we analyze the CyberCIEGE game [10] as part of our study. When starting any game, it is necessary to examine not only the gameplay, but also the various objectives or missions that are offered. When loading CyberCIEGE, a starting menu is shown that includes the various scenarios that are available, as seen in Figure 1. Thus, from here we can figure out some of the potential topics that


Fig. 1. CyberCIEGE game: starting menu.

Fig. 2. CyberCIEGE gameplay screenshot 1.

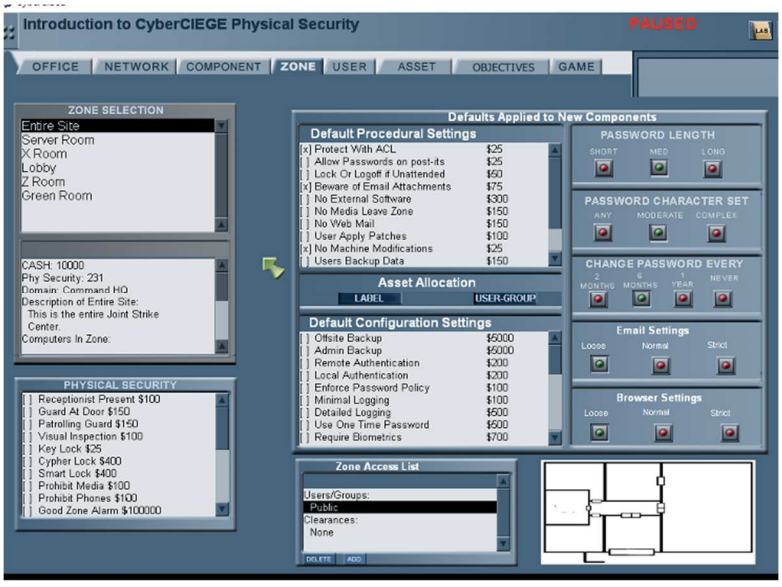


Fig. 3. The CyberCIEGE cybersecurity educational game scenario-based play screenshot 2.

| | *Anti-Phishing Phil | *Cyber Awareness Challenge | *CyberCIEGE | *Cyber Protect | *PASDJO | *What.Hack | *CyberStart Go | *Facebook CTF | *DEFCON | *Mozilla | *RuCTFe | *picoCTF | *Bandit OverTheWire | *Education Arcade |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Knowledge Area**: Knowledge Unit | **Data Security**: Data Integrity and Authentication<br>**Human Security**: Social Engineering | **Data Security:** Data Integrity and Authentication, Access Control<br>**System Security:** System Access, System Control<br>**Human Security:** Social Engineering | **Data Security:** Data Integrity and Authentication, Access Control<br>**Software Security:** Implementation<br>**Connection Security:** Network Defense<br>**System Security:** System Access, System Control<br>**Human Security:** Social Engineering, Identity Management<br>**Organizational Security:** Social Engineering | **Data Security:** Data Integrity and Authentication, Access Control<br>**Software Security:** Implementation<br>**Connection Security:** Network Defense<br>**System Security:** System Access, System Control<br>**Human Security:** Social Engineering<br>**Organizational Security:** Social Engineering | **Data Security:** Data Integrity and Authentication<br>**System Security:** System Access<br>**Human Security:** Awareness and Understanding | **Data Security** Data Integrity and Authentication<br>**Human Security** Social Engineering<br>**Organizational Security** Risk Management<br>**Societal Security** Cybercrime | **Data Security** Cryptography, Digital Forensics, Data Integrity and Authentication<br>**System Security** System Access<br>**Human Security** Identity Management<br>**Software Security** Implementation | **Data Security** Data Integrity and Authentication, Access Control<br>**Software Security** Implementation<br>**System Security** System Access, System Control | **Data Security** Data Integrity and Authentication<br>**Software Security** Implementation<br>**System Security** System Access<br>**Human Security** Identity Management | **Data Security** Data Integrity and Authentication, Digital Forensics<br>**Software Security** Implementation<br>**System Security** System Testing<br>**Human Security** Social Engineering | **Data Security** Data Integrity and Authentication<br>**Component Security** Component Reverse Engineering<br>**Human Security** Awareness and Understanding | **Data Security** Digital Forensics, Access Control<br>**Component Security** Component Reverse Engineering<br>**System Security** System Access, System Control | **Data Security** Data Integrity and Authentication<br>**Software Security** Implementation<br>**System Security** System Control | **Data Security** Data Integrity and Authentication, Access Control<br>**System Security** System Access, System Control<br>**Human Security** Identity Management, Social Engineering<br>**Societal Security** Cybercrime |

**Table 1. CSEC2017 Analysis Results:** *These CSEC2017 curricular reference-based assessment outcomes are obtained by conceptual mapping of our surveyed cybersecurity educational games to the CSEC2017 Knowledge Areas (KA s) based upon the KA s covered in each game, as well as the Knowledge Units (KU s) covered within each KA. The games, whose CSEC2017 alignment we study here, are intended for college-level audiences. Games with an asterisk (*) are intended for multiple audiences.*

| | *Anti-Phishing Phil | *Cyber Awareness Challenge | *CyberCIEGE | *Cyber Protect | *CyberStart Go | *Facebook CTF | *DEFCON | *Mozilla | *RuCTFe | *picoCTF | *Bandit OverTheWire | *Education Arcade |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Workforce Function**: Specialty Area – *Work Role* | **Analyze**: Exploitation Analysis – *Exploitation Analyst*<br>**Protect and Defend**: Cyber Defense Analysis – *Cyber Defense Analyst* | **Protect and Defend**: Incident Response – *Cyber Defense Incident Response*<br>**Oversee and Govern**: Training Education and Awareness – *Cyber Instructor* | **Operate and Maintain**: Systems Analysis – *Systems Analyst*<br>**Oversee and Govern**: Cybersecurity Management – *Information Systems Security Manager*<br>**Protect and Defend**: Vulnerability Assessment and Management – *Vulnerability Assessment Analyst*<br>**Securely Provision:** Risk Management – *Authorizing Official/Designating Representative* | **Operate and Maintain**: Systems Administration – *Systems Administrator*<br>**Oversee and Govern** Cybersecurity Management – *Information Systems Security Manager*<br>**Protect and Defend** Cyber Defense Analysis – *Cyber Defense Analyst*<br>**Securely Provision:** Risk Management – *Authorizing Official/Designating Representative* | **Investigate** Digital Forensics – *Cyber Defense Forensics Analyst*<br>**Oversee and Govern** Training Education and Awareness – *Cyber Instructor* | **Securely Provision** Software Development – *Secure Software Assessor*<br>**Oversee and Govern** Cybersecurity Management – *Information Systems Security Manager* | **Protect and Defend** Cyber Defense Analysis - *Cyber Defense Analyst*<br>**Collect and Operate** Cyber Operations – *Cyber Operator*<br>**Analyze** Exploitation Analysis – *Exploitation Analyst* | **Protect and Defend** Cyber Defense Infrastructure Support - *Cyber Defense Infrastructure Support Specialist*<br>**Collect and Operate** Cyber Operational Planning - *Cyber Operations Planner*<br>**Analyze** Exploitation Analysis - *Exploitation Analyst*<br>**Investigate** Digital Forensics - *Forensics Analyst* | **Protect and Defend** Cyber Defense Analysis - *Cyber Defense Analyst*<br>**Collect and Operate** Cyber Operations – *Cyber Operator*<br>**Analyze** Exploitation Analysis – *Exploitation Analyst*<br>**Operate and Maintain** Systems Analysis. – *Systems Security Analyst* | **Investigate** Digital Forensics – *Cyber Defense Forensics Analyst*<br>**Analyze** All-source Analysis – *All-source Analyst*<br>**Collect and Operate** Cyber Operations – *Cyber Operator* | **Oversee and Govern** Cybersecurity Management – *Information Systems Security Manager*<br>**Analyze** Exploitation Analysis – *Exploitation Analyst* | **Oversee and Govern** Training Education and Awareness – *Cyber Instructor*<br>**Analyze** Exploitation Analysis – *Exploitation Analyst* |

**Table 2. NICE Analysis Results:** *These NICE framework-based assessment outcomes are obtained by conceptual mapping of our surveyed cybersecurity educational games to the workforce functions covered in each game, as well as the specialty areas and work roles covered within each workforce function. These games, which we analyzed here, is intended for industry-level audience i.e., college graduates. Games with an asterisk (*) are intended for multiple audiences.*

this game will teach the user about. Once loaded into the first scenario, the game's aspects can be further examined. Upon exploring the different scenario content areas available within the game, as shown in Figures 2 and 3, prior to completing the objectives, it is clear that the game covers multiple topics, including phishing, authentication, access control and passwords. After the initial observations, we then focus on completing the objectives, including taking note of the content topics that are taught. This process is repeated until all, or as many possible game play scenarios are completed. In an attempt to remain thorough and consistent in our conceptual analysis, we map every topic included in each game, whether it is mentioned in only one section of the game, or it is covered or discussed throughout the game.

## IV. Our Analysis Results For Cybersecurity Educational Games

For making our mapping more practical, meaningful and useful, we analyzed each cyber educational game based on the intended audience. The CSEC2017 is primarily intended for post-secondary users, the NICE Framework is intended for industry-level users, the CATS framework topics are intended for college-level students, and the GenCyber concepts are intended for K-12 community users. We determined the intended audience for each game by referring to the original source point of each game came and by referring to existing literature on these games. Tables 1, 2, 3 and 4 display our conceptual mapping based analysis results

| | *Anti-Phishing Phil | *Cyber Awareness Challenge | *CyberCIEGE | *Cyber Protect | *PASDJO | *What.Hack | *CyberStart Go | *Facebook CTF | *DEFCON | *Mozilla | *RuCTFe | *picoCTF | *Bandit OverTheWire | *Education Arcade |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Cybersecurity Concept Inventory (CCI) Topics** | Identity attacks against CIA triad and authentication<br>Identify possible phishing emails from a set of samples | Identify attacks against CIA triad and Authentication<br>Identify Risky Behaviors | Identify vulnerabilities and failures<br>Devise a defense<br>Identify risky behaviors<br>Devise security plan<br>Identify possible phishing emails from a set of samples | Identify vulnerabilities and failures<br>Identify attacks against CIA triad and authentication<br>Devise a defense<br>Explain why a failure happened<br>Devise a security plan<br>Identify a vulnerability in software | Identify risky behaviors<br>Identify a vulnerability | Identify risky behaviors<br>Identify possible phishing emails from a set of samples | Identify Risky Behaviors<br>Identify Vulnerabilities in Software | Devise an attack<br>Solve a puzzle requiring "out-of-the-box" thinking | Identify Vulnerabilities and failures<br>Identify attacks against CIA triad and Authentication<br>Devise an attack<br>Explain how to exploit a software vulnerability | Identify vulnerabilities and failures<br>Identify attacks against CIA triad and Authentication<br>Identify which assumptions of a system are most likely to be exploitable | Identify attacks against CIA triad and Authentication<br>Identify which assumptions of a system are most likely to be exploitable<br>Explain how to exploit a software vulnerability | Identify potential targets and attackers | Explain how to exploit a software vulnerability | Identify attacks against CIA triad and Authentication<br>Identify risky behaviors<br>Identify a vulnerability<br>Identify possible phishing emails from a set of samples |
| **Cybersecurity Curriculum Assessment (CCA) Topics** | Integrity<br>Confidentiality<br>Manage Risks<br>Social Engineering | Authentication<br>Confidentiality<br>Manage Risks<br>Insider Threat<br>Access Control<br>Incident Analysis | Authentication<br>Integrity<br>Confidentiality<br>Analyze Threats<br>Manage Risks<br>Access Control<br>Social Engineering<br>Design Secure Protocols<br>Incident Analysis | Integrity<br>Assess vulnerabilities<br>Social Engineering<br>Insider Threat<br>Access Control<br>Design and Analyze Secure Networks<br>Software Vulnerability Analysis | Authentication | Analyze threats<br>Manage Risks<br>Social Engineering | Authentication<br>Operating System Security<br>Software Vulnerability Analysis | Authentication<br>Secure Coding | Assess vulnerabilities<br>Well known attacks, such as man-in-the-middle | Confidentiality<br>Assess vulnerabilities<br>Social engineering<br>Software vulnerability analysis<br>Design and analyze secure web applications | Assess vulnerabilities<br>Software vulnerability analysis | Analyze threats<br>Forensics<br>Design and analyze secure web applications | Scripting languages, systems programming, low-level programming<br>Applications of homomorphic encryption and private information retrieval<br>Secure coding | Authentication<br>Integrity<br>Confidentiality<br>Assess Vulnerabilities<br>Manage Risks |

**Table 3. CATS Analysis Results:** *Here, we use the Cybersecurity Assessment Tools (CATS) to analyze our list of cybersecurity educational games by mapping every one of them to the list of Cybersecurity Concept Inventory (CCI) topics and the Cybersecurity Curriculum Assessment (CCA) topic, as covered in each game. The list of game, which we surveyed using the CATS framework, is intended for college-level audiences. Games with an asterisk (*) are intended for multiple audiences.*

| | *Anti-Phishing Phil | *CyberCIEGE | Nsteens | OnGuardOnline | NOVA Labs | Safe Online Surfing | Interland | *Education Arcade | Targeted Attack: The Game | The Missing Link: A Cybersecurity Mystery | Aggie LIFE |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **GenCyber Security-First Concepts** | Confidentiality<br>Integrity<br>Think Like an Adversary | Defense in Depth<br>Confidentiality<br>Integrity<br>Think Like an Adversary | Integrity<br>Think Like an Adversary | Integrity<br>Confidentiality | Defense in Depth<br>Integrity<br>Think Like an Adversary | Integrity<br>Confidentiality<br>Think Like an Adversary | Integrity<br>Think Like an Adversary | Confidentiality<br>Think Like an Adversary<br>Integrity | Defense in Depth<br>Confidentiality<br>Integrity<br>Think Like an Adversary | Integrity<br>Think Like an Adversary | Defense in Depth<br>Confidentiality |

**Table 4. GenCyber Analysis Results:** *These assessment outcomes are produced by mapping our list of surveyed cybersecurity educational games to the GenCyber security-first concepts i.e., by determining the list of GenCyber cybersecurity concepts covered in each game. The list of games, which we analyzed using the GenCyber concepts, is intended for K-12 audiences. Games with an asterisk (*) are intended for multiple audiences.)*

using each of our selected benchmarks. In each table, we have marked those games with an asterisk that are intended for multiple audiences.

Table 1 shows the results of our conceptual mapping of the games intended for a college-level audience using CSEC2017. We analyzed each game in terms of its coverage of the KA s and KU s. Previous taxonomy based mapping studies in cybersecurity education, that have utilized CSEC2017, have only used the KA s. However, our work goes a step further by also accounting for the KU s in addition to the KA s. This enables us to analyze more in-depth on the specific topics that are covered. The results from this table can be used to determine which games could be used to teach specific KA s and/or KU s at the college level.

Table 2 displays our analysis results from the usage of the NICE Framework. We analyzed each game in terms of Workforce Functions, as well as the Specialty Area and Work Role within each Workforce Function, as covered in each game. The results from this can be potentially helpful to those from the industry, or to those, who are entering the cybersecurity workforce, as they could be used to determine how these games could be utilized in the advanced level game-based training for various cybersecurity job positions.

Table 3 exhibits our conceptual mapping results based upon the CATS assessment framework components - CCI and CCA. Both the CCI topics and the CCA topics are intended for college-level students, and be useful in terms of training & assessing the students on those basic cybersecurity topics that they need to know as starters plus as graduates. This could also be used to determine which games can be utilized to teach the corresponding mapped CCI and CCA topics to college students.

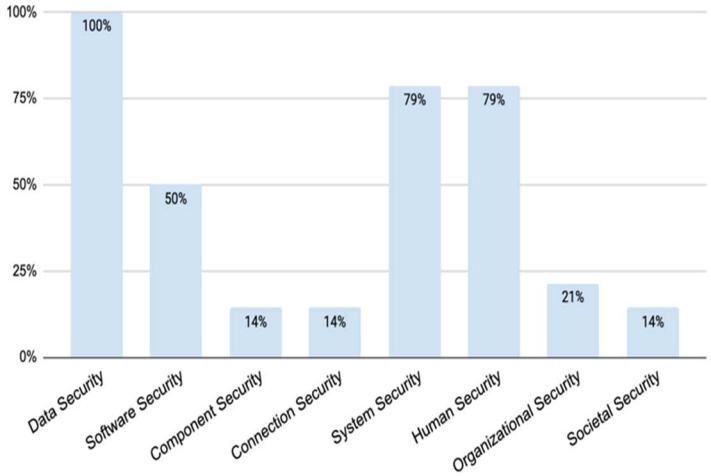


Fig. 4. The extent to which (in terms of percentage) each CSEC2017 knowledge areas (KA) is covered in the list of popular cybersecurity educational games that we analyzed.

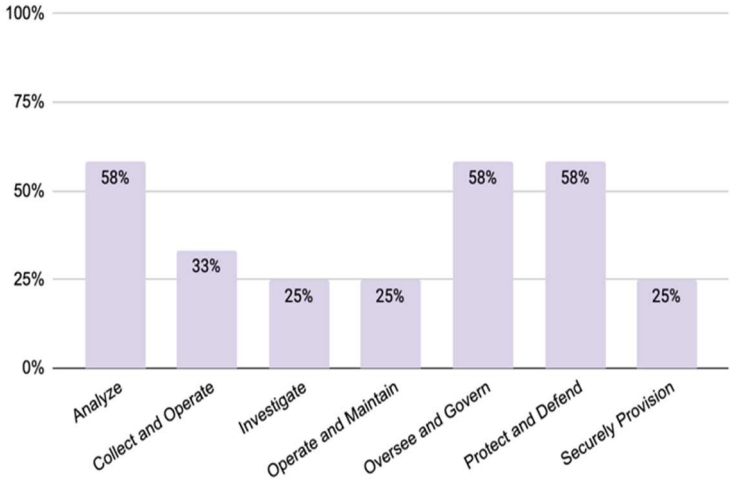


Fig. 5. The extent to which (in terms of percentage) each NICE workforce function is covered in the list of popular cybersecurity educational games that we assessed.

Last, but not the least, Table 4 lists the results from our conceptual mapping with the GenCyber concepts. This table is intended for a K-12 audience, and can be useful to the pre-college community to find out which cybersecurity concepts are covered by the K-12 level cybersecurity education games.

## V. Gap Analysis

In addition to our conceptual mapping based analysis using the chosen benchmarks, we also performed a gap analysis, as part of our study, in which we determine the topics in each framework that are covered, as well as highlight the topics that are not covered or are lacking coverage. Our unique approach of taxonomy building for cyber educational games not only provides us a medium for analyzing the strength in terms of alignments or coverage of topics from each reference framework, which is used in our

conceptual mapping, but for also finding out the weaknesses (or gaps) in terms of non-alignment or non-coverage. This sort of holistic analysis moreover assists us in comparing one cybersecurity educational game to another one in terms of what one offers in educational content value compared to another. A recent work [47] illustrates an academic benchmark based taxonomy framework for comparing one computer science educational course (or module) to another. However, to our knowledge there is no previous instance of work that demonstrates such use of a conceptual analysis, based upon academic & industry benchmarks, to compare cybersecurity educational games.

As part of our additional gap analsyis study, Figure 4 shows the extent to which each CSEC2017 KA was found covered in our selected set of cybersecurity educational games that were analyzed. As seen from the figure, the Data Security KA was observed in all of the games that were analyzed making it the most string coverage area (or topic). The System Security and Human Security KA s were mapped to a majority of the analyzed games. The Software Security

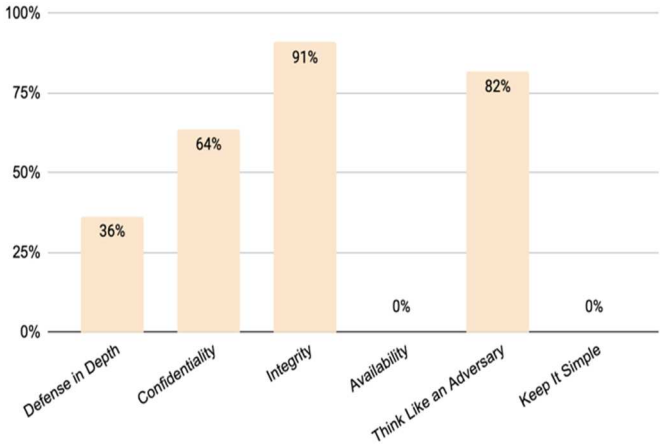


Fig. 6. The extent to which (in terms of percentage) each GenCyber cybersecurity concept is covered in the list of popular cybersecurity educational games that we surveyed.

KA was covered in half of the analyzed games. Lastly, the KA s lacking coverage were Component Security, Connection Security, Organizational Security, and Societal Security, thus making them the weak areas, or gaps within,

Figure 5 depicts the extent to which each NICE Framework Workforce Function was mapped to in our list of analyzed games. The Analyze, Oversee & Govern, and Protect & Defend Workforce Functions were covered in about half of the analyzed games making them the area of strength. The Workforce Functions lacking coverage included Collect & Operate, Investigate, Operate & Maintain, and Securely Provision, thus making them the areas of weakness (or gap).

Figure 6 indicates the extent of coverage of GenCyber Concepts in the set of analyzed games. The Integrity concept is observed in almost all of the games, thus making it the strength in terms of coverage. The Confidentiality and Adversarial Thinking concepts are seen to be covered in a majority of the games. The Defense in Depth concept, on the other hand, has less coverage compared to the other concepts, while Availability and Keep It Simple received no coverage at all, thus making it the area of weakness (or gap) .

Thus, this gap analysis, which results from our study of the cybersecurity educational games, can further provide valuable information on what are the weaknesses in each game that need to be addressed, or the gaps to be filled. The visual graphs hat we were able to generate from our analysis results can provide useful insights, and become a vital resource to the cybersecurity game creators in improving these games by filling in the missing content areas or gaps.

## VI. CONCLUSION

It is noteworthy that the use of academic benchmarks and industry frameworks for conceptual taxonomy building within cybersecurity education is not new [25, 28, 31, 41, 42]. However, it is novel for traditional cybersecurity educational games, and that's where our primary research contribution lies in this paper. Previous research done on cybersecurity educational games have mainly focused on learner performance, effectiveness and engagement. To our knowledge, there is no prior published survey work done on the exclusive analysis of how these games fare in terms of their alignment with standard academic benchmarks and industry job related demands. The closest and most relevant work in this regard within existing literature on cyber educational games only proposes a conceptual framework [33] consisting of learning theories and training models, plus some industry benchmarks, but does not share the results of its application towards games. This paper intends to fill in this research gap in the context of cybersecurity educational games.

Our work is novel in the sense it demonstrates conceptual analysis based mapping of traditional cybersecurity games to a set of carefully chosen academic plus industry benchmarks, which are developed by professionals in the cybersecurity field. Our work provides different stakeholders, including the K-12 cybersecurity educators, the college-level academic community, and industry users valuable insights in regard to making a choice with these games for educational and training settings. By using multiple frameworks and mapping each game based on the intended audience(s), our results give more relevant and meaningful information to the user. Additionally, our gap analysis results provide insights into the extent to which different cybersecurity content topics or area are covered in a set of selected games, as well as assist the game developers with future scope of improvement and enhancements to the cybersecurity educational games.

Our results are a potential resource for cybersecurity educators, the academic community, and industry members alike. Our insights and specialized information could be used to help implement cybersecurity educational games into academic programs and industry training as a way to improve

comprehension and awareness in a diverse set of education areas. In addition, our results could be used as a resource for those involved in recreational gaming, who want to further explore the realm of cybersecurity.

As a future extension of this work, we would also like to expand the list of cyber educational games that we have analyzed in this research study. We would also like to add other industry reference frameworks and application domains (like the National Cyber League knowledge domain areas, the Cyber Kill Chain framework, and the MITRE organizational frameworks on cybersecurity) to our list of benchmarks for added analysis results. We also intend to incorporate the latest, revised NICE framework for our future studies. We hope to make our survey results a comprehensive repository for all cyber educational games.

## VII. REFERENCES


[1] D. L. Burley et al., "Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity," *Association for Computing Machinery (ACM)*, Dec. 2017, doi: 10.1145/3184594.

[2] "GenCyber." www.gen-cyber.com/ (accessed February 2021).

[3] G. Jin, M. Tu, T. Kim, J Heffron, J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Student" *Journal of Education and Learning (EduLearn)*, vol. 12, no. 1, pp. 150-158, Feb. 2018, doi: 10.11591/edulearn.v12i1.7736.

[4] S. Kucek and M. Leitner, "An Empirical Survey of Functions and Configurations of Open-Source Capture the Flag (CTF) Environments," *Journal of Network and Computer Applications*, vol. 151, Feb. 2020, doi: 10.1016/j.jnca.2019.102470.

[5] W. Newhouse, S. Keith, B. Scribner, G. Witte, "National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework," *National Institute of Standards and Technology*, Aug. 2017, doi: 10.6028/NIST.SP.800-181.

[6] A. Sherman et al., "Creating a Cybersecurity Concept Inventory: A Status Report on the CATS Project," *National Cyber Summit*, June 2017.

[7] J. Tioh, M. Mina, D.W. Jacobson, "Cyber Security Training a Survey of Serious Games in Cyber Security," *2017 IEEE Frontiers in Education Conference (FIE)*, pp. 1-5, Oct. 2017, doi: 10.1109/FIE.2017.8190712.

[8] "Anti-Phishing Phil." https://www.ucl.ac.uk/cert/antiphishing/ (accessed February 2021).

[9] "Cyber Awareness Challenge." https://public.cyber.mil/training/cyber-awareness-challenge/ (accessed February 2021)

[10] "Cyber CIEGE." https://nps.edu/web/c3o/downloads (accessed July 14, 2021)

[11] "CyberProtect." https://pipaliya.com/cyber-protect/launchpage.html (accessed February 2021)

[12] "Nsteens." https://www.nsteens.org/Games (accessed February 2021)

[13] "NOVA Labs." https://www.pbs.org/wgbh/nova/labs/lab/cyber/ (accessed July 15, 2021)

[14] "What.Hack." https://gdiac.cs.cornell.edu/zkwen/whatdothack/ (accessed February 2021)

[15] "PASDJO." https://password-game.firebaseapp.com/ (accessed February 2021)

[16] "CyberStart Go." https://go.joincyberstart.com (accessed July 15, 2021)

[17] "OnGuardOnline." https://www.consumer.ftc.gov/features/feature-0038-onguardonline (accessed February 2021)

[18] "Safe Online Surfing." https://sos.fbi.gov/en/ (accessed June 18, 2021)

[19] "Interland." https://beinternetawesome.withgoogle.com/en/interland (accessed July 15, 2021)

[20] A. Le Compte, D. Elizondo, and T. Watson, "A Renewed Approach to Serious Games for Cyber Security," *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 203-216, 2015, doi: 10.1109/CYCON.2015.7158478.

[21] F. Tchakounté, L. K. Wabo, and M. Atemkeng, "A Review of Gamification Applied to Phishing," 10.20944/preprints202003.0139.v1.

[22] F. Alotaibi, S. Furnell, I. Stengel, and M. Papadaki, "A review of using gaming technology for cyber-security awareness," *International Journal for Information Security Research (IJISR),* vol. 6, no. 2, pp. 660-666, June 2016, doi: 10.20533/ijisr.2042.4639.2016.0076.

[23] R. Raman, S. Sunny, V. Pavithran, and K. Achuthan, "Framework for evaluating Capture The Flag (CTF) security competitions," *IEEE International Conference for Convergence for Technology*, pp. 1-5, Apr. 2014, doi: 10.1109/I2CT.2014.7092098.

[24] M. Hendrix, A. Al-Sherbaz, and V. Bloom, "Game based cyber security training: are serious games suitable for cyber security training?" *International Journal of Serious Games*, vol. 3, no. 1, pp. 53-61, Jan. 2016, doi: 10.17083/ijsg.v3i1.107.

[25] J. Hallett, R. Larson, and A. Rashid, "Mirror, mirror, on the wall: What are we teaching them all? Characterizing the focus of cybersecurity curricular frameworks," *USENIX Workshop on Advances in Security Education*, Aug. 2018.

[26] P. Gestwicki, and K. Stumbaugh, "Observations and opportunities in cybersecurity education game design," *The 20th International Conference on Computer Games*, pp. 131-137, 2015, doi: 10.1109/CGames.2015.7272970.

[27] R. Roepke, and U. Schroeder, "The Problem with Teaching Defence against the Dark Arts: A Review of Game-based Learning Applications and Serious Games for Cyber Security Education," *The 11th International Conference on Computer Supported Education*, pp. 58-66, 2019, doi: 10.5220/0007706100580066.

[28] M. Gondree, Z. N. Peterson, and P. Pusey, "Talking about Talking about Cybersecurity Games," *login Usenix Mag.*, vol. 41, no. 1, 2016.

[29] M. H. bin Noor Azam, and R. Beuran, "Usability Evaluation of Open Source and Online Capture the Flag Platforms."

[30] H. Gonzalez, R. Llamas, and O. Montano, "Using CTF Tournament for Reinforcing Learned Skills in Cybersecurity Course," *Research in Computing Science*, vol. 148, no. 5, pp. 133-141, 2019, doi: 10.13053/rcs-148-5-15.

[31] M. Kranch, "Why You Should Start with the Offense: How to Best Teach Cybersecurity's Core Concepts," *Colloquium for Information Systems Security Education*, vol. 23, no.1, pp. 1-12, June 2019.

[32] Y. Wang, Y. Wang, J. Liu, Z. Huang, and P. Xie, "A survey of game theoretic methods for cyber security," *IEEE First International Conference on Data Science in Cyberspace*, pp. 631-636, 2016, doi: 10.1109/DSC.2016.90.

[33] N.M. Katsantonis, I. Kotini, P. Fouliras, and I. Mavridis, "Conceptual framework for developing cyber security serious games," *IEEE Global Engineering Education Conference*, pp. 872-881, 2019, doi: 10.1109/EDUCON.2019.8725061.

[34] G. Jin, M. Tu, T. H. Kim, J. Heffron, and J. White, "Game based cybersecurity training for high school students," *The 49th ACM Technical Symposium on Computer Science Education*, pp. 68-73, Feb. 2018, doi:10.1145/3159450.3159591.

[35] L. J. Khoo, "Design and Develop a Cybersecurity Education Framework Using Capture the Flag (CTF)," *Design, Motivation, and Frameworks in Game-Based Learning*, pp. 123-153, 2019, doi:10.4018/978-1-5225-6026-5.CH005.

[36] M. Beltrán, M. Calvo, and S. González, "Experiences using capture the flag competitions to introduce gamification in undergraduate computer security labs," *International Conference on Computational Science and Computational Intelligence*, pp. 574-579, 2018, doi: 10.1109/CSCI46756.2018.00116.

[37] M. Ahmad, "Categorizing Game Design Elements into Educational Game Design Fundamentals," *Game Design and Intelligent Interaction*, Nov. 2019, doi: 10.5772/intechopen.89971.

[38] M. Maarek, S. Louchart, L. McGregor, and R. McMenemy, "Co-created Design of a Serious Game Investigation into Developer-Centred Security," *International Conference on Games and Learning Alliance*, pp. 221-231, 2018, doi: 10.1007/978-3-030-11548-7_21.

[39] C. Taylor, P. Arias, J. Klopchic, C. Matarazzo, and E. Dube, "CTF: State-of-the-Art and Building the Next Generation," *USENIX Workshop on Advances in Security Education*, Aug. 2017.

[40] S. M. T. Toapanta, J. M. E. Jaramillo, and L. M. E. Gallegos, "Cybersecurity analysis to determine the impact on the social area in Latin America and the Caribbean," *2nd International Conference on Education Technology Management*, pp. 73-78, Dec. 2019, doi: 10.1145/3375900.3375911.

[41] M. Katsantonis, and I. Mavridis, "Ontology-Based Modelling for Cyber Security E-Learning and Training," *International Conference on Web-Based Learning*, pp. 15-27, 2019, doi :10.1007/978-3-030-35758-0_2.

[42] V. Švábenský, J. Vykopal, and P. Čeleda, "What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences," *51st ACM Technical Symposium on Computer Science Education*, pp. 2-8, Feb. 2020, doi: 10.1145/3328778.3366816.

[43] "Targeted Attack: The Game." http://targetedattacks.trendmicro.com/ (accessed July 15, 2021)

[44] "The Missing Link: A Cybersecurity Mystery." https://it.tamu.edu/missinglink/ (accessed July 15, 2021)

[45] "Aggie LIFE." https://it.tamu.edu/aggielife/ (accessed February 2021)

[46] "Education Arcade." https://www.educationarcade.co.nz/game-time (accessed February 2021)

[47] "CS Materials." https://cs-materials.herokuapp.com/ (accessed April 2021).

[48] V. Švábenský, P. Čeleda, J. Vykopal, and S. Brišáková, "Cybersecurity knowledge and skills taught in capture the flag challenges," *Computers & Security*, *102*, 102154, Mar. 2021.