EFFECTS OF A GAME-BASED CYBERSECURITY SKILL TRAINING IN LEARNING CYBERSECURITY AMONG UNDERGRADUATES

KHOO LI JING

SULTAN IDRIS EDUCATION UNIVERSITY

2025

EFFECTS OF A GAME-BASED CYBERSECURITY SKILL TRAINING IN LEARNING CYBERSECURITY AMONG UNDERGRADUATES

KHOO LI JING

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

THESIS PRESENTED TO QUALIFY FOR A DOCTOR OF PHILOSOPHY

FACULTY OF ART, SUSTAINABILITY AND CREATIVE INDUSTRY
SULTAN IDRIS EDUCATION UNIVERSITY

2025

05-4506832 pustaka.upsi.edu.my Perpustakaan Tuanku Bainun Kampus Sultan Abdul Jalil Shah PustakaTBainun ptbupsi

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

Sila tanda (√)

Kertas Projek	
Sarjana Penyelidikan	
Sarjana Penyelidikan dan Kerja Kursus	
Doktor Falsafah	✓

INSTITUT PENGAJIAN SISWAZAH

PERAKUAN KEASLIAN PENULISAN

Perakuan ini telah dibuat pada 15 (hari bulan) April (bulan) 2025

i. Perakuan pelajar :

Saya, Khoo Li Jing, P20142001247, Fakulti Seni, Komputeran dan Industri Kreatif (SILA NYATAKAN NAMA PELAJAR, NO. MATRIK DAN FAKULTI) dengan ini mengaku bahawa disertasi/tesis yang bertajuk Effects Of A Game-Based Cybersecurity Skill Training In Learning Cybersecurity Among Undergraduates

adalah hasil kerja saya sendiri. Saya tidak memplagiat dan apa-apa penggunaan mana-mana hasil kerja yang mengandungi hak cipta telah dilakukan secara urusan yang wajar dan bagi maksud yang dibenarkan dan apa-apa petikan, ekstrak, rujukan atau pengeluaran semula daripada atau kepada mana-mana hasil kerja yang mengandungi hak cipta telah dinyatakan dengan sejelasnya dan secukupnya

Tandatangan pelajar

ii. Perakuan Penyelia:

Saya, Prof. Madya Dr. Ing Maizatul Mohamad Yatim (NAMA PENYELIA) dengan ini mengesahkan bahawa hasil kerja pelajar yang bertajuk Effects Of A Game-Based Cybersecurity Skill Training In Learning Cybersecurity Among Undergraduates

(TAJUK) dihasilkan oleh pelajar seperti nama di atas, dan telah diserahkan kepada Institut Pengajian Siswazah bagi memenuhi sebahagian/sepenuhnya syarat untuk memperoleh Ijazah Doktor Falsafah (Pembelajaran Berasaskan Permainan) (SLA NYATAKAN NAMA IJAZAH).

15 April 2025
Tarikh

Tandatangan Penyelia

UPSI/IPS-3/BO 31
Pind.: 01 m/s:1/1

UNIVERSITI PENDIDIKAN SULTAN IDRIS
SULTAN IDRIS EDUCATION UNIVERSITY

INSTITUT PENGAJIAN SISWAZAH /
INSTITUTE OF GRADUATE STUDIES

BORANG PENGESAHAN PENYERAHAN TESIS/DISERTASI/LAPORAN KERTAS PROJEK
DECLARATION OF THESIS/DISSERTATION/PROJECT PAPER FORM

Tajuk / *Title*: Effects Of A Game-Based Cybersecurity Skill Training In Learning Cybersecurity Among Undergraduates

No. Matrik /*Matric's No.*: P20142001247

Saya / *I* : Khoo Li Jing

(Nama pelajar / *Student's Name*)

mengaku membenarkan Tesis/Disertasi/Laporan Kertas Projek (Kedoktoran/Sarjana)* ini disimpan di Universiti Pendidikan Sultan Idris (Perpustakaan Tuanku Bainun) dengan syarat-syarat kegunaan seperti berikut:-
acknowledged that Universiti Pendidikan Sultan Idris (Tuanku Bainun Library) reserves the right as follows:-

1. Tesis/Disertasi/Laporan Kertas Projek ini adalah hak milik UPSI.
   The thesis is the property of Universiti Pendidikan Sultan Idris
2. Perpustakaan Tuanku Bainun dibenarkan membuat salinan untuk tujuan rujukan dan penyelidikan.
   Tuanku Bainun Library has the right to make copies for the purpose of reference and research.
3. Perpustakaan dibenarkan membuat salinan Tesis/Disertasi ini sebagai bahan pertukaran antara Institusi Pengajian Tinggi.
   The Library has the right to make copies of the thesis for academic exchange.
4. Sila tandakan (√) bagi pilihan kategori di bawah / *Please tick (√) for category below:-*

☐ **SULIT/*CONFIDENTIAL*** — Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub dalam Akta Rahsia Rasmi 1972. / *Contains confidential information under the Official Secret Act 1972*

☐ **TERHAD/*RESTRICTED*** — Mengandungi maklumat terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan ini dijalankan. / *Contains restricted information as specified by the organization where research was done.*

☑ **TIDAK TERHAD / *OPEN ACCESS***

(Tandatangan Pelajar/ Signature)

Tarikh: 15 April 2025

(Tandatangan Penyelia / *Signature of Supervisor*)
& (Nama & Cop Rasmi / *Name & Official Stamp*)

Prof. Madya Dr. Ing Maizatul Hayati Mohamad Yatim
Penyarah
Fakulti Komputeran dan Meta-Teknologi
Universiti Pendidikan Sultan Idris
35900 Tanjong Malim, Perak

Catatan: Jika Tesis/Disertasi ini **SULIT @ TERHAD**, sila lampirkan surat daripada pihak berkuasa/organisasi berkenaan dengan menyatakan sekali sebab dan tempoh laporan ini perlu dikelaskan sebagai **SULIT** dan **TERHAD**.

Notes: If the thesis is CONFIDENTAL or RESTRICTED, please attach with the letter from the organization with period and reasons for confidentiality or restriction.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to my supervisor Assoc. Prof. Dr. –Ing. Maizatul Hayati Mohamad Yatim for her unwavering guidance, expertise, and continuous support throughout the entire duration of this thesis. I am also indebted to my second supervisor, Assoc. Prof. Dr. Tan Wee Hoe, for his valuable input and advice, which have significantly contributed to the quality of this work. Their invaluable insights and constructive feedback have been instrumental in shaping and refining my research.

I would like to extend my heartfelt appreciation to the participating universities, University Pendidikan Sultan Idris (UPSI) and University of Wollongong Malaysia (UOWM), for providing the necessary resources and research opportunities that enabled me to undertake this study. The collaborative environment fostered by these institutions has been instrumental in broadening my knowledge and enhancing the quality of my research.

Lastly, I would like to express my deepest gratitude to my beloved family for their unwavering love, encouragement, and understanding. Their constant support and belief in my abilities have been the driving force behind my success. Their sacrifices and unconditional love have given me the strength to overcome challenges and pursue my academic goals.

ABSTRACT

This research investigates the effectiveness of a Capture the Flag (CTF) game-based training module in enhancing students' understanding of cybersecurity concepts. The primary issue addressed is the gap in practical cybersecurity skills among students, despite theoretical knowledge. To tackle this, we developed a CTF web-based game called *Script Kiddie Resilience Capture the Flag* (SKRCTF) using a five-step gamification approach tailored for educational purposes. The game design process began with aligning the cybersecurity education syllabus from two universities with industry standards. This alignment ensured relevance and applicability. We then deployed a minimum viable prototype (MVP) of the game on an e-learning platform, guided by the Technological Pedagogical and Content Knowledge (TPACK) framework. The game's Pedagogical Content Knowledge (PCK) was validated by four experienced academicians, and its Technology Content Knowledge (TCK) was assessed by two cybersecurity professionals. The game impact was tested on 71 university students through a quasi-experimental design, featuring non-equivalent control groups with pre-test and post-test assessments. Students were divided into cohorts within an academic semester, with the experimental group engaging with the SKRCTF game. Initial results after 12 weeks showed no significant improvement in the experimental group's ability to recognize cybersecurity threats and cryptography patterns. This led to the formulation of 22 null hypotheses regarding the game's effect on novice learners in cybersecurity. In response to these findings, we adjusted the game's guides and challenges and conducted a second experiment. This iteration revealed a slight improvement in participants' abilities to calculate basic cryptographic algorithms and recognize simple malicious code. In conclusion, the research underscores the importance of foundational computer science knowledge, such as operating systems, networking, and programming, for effective learning in cybersecurity. Our findings highlight the cognitive skills necessary for students before engaging in advanced cybersecurity training and demonstrate the nuanced impact of game-based learning on acquiring cybersecurity skills.

KESAN LATIHAN KEMAHIRAN KESELAMATAN SIBER BERASASKAN PERMAINAN DALAM PEMBELAJARAN KESELAMATAN SIBER DALAM KALANGAN PRA SISWAZAH

ABSTRAK

Kajian ini dijalankan untuk mengesahkan latihan berasaskan permainan *Capture the Flag* (CTF) sebagai latihan kemahiran keselamatan siber ke arah pemahaman pelajar tentang konsep keselamatan siber. Permainan berasaskan web bertajuk *Script Kiddie Resilience Capture the Flag* (SKRCTF) telah dibangunkan sebagai contoh kes dengan menggunakan pendekatan Gamifikasi Lima Langkah Dalam Pendidikan. Reka bentuk permainan bermula dengan penjajaran konstruktif terhadap sukatan pelajaran pendidikan keselamatan siber yang diajar di dua buah universiti dan mematuhi piawaian industri. Kemudian, pembangunan permainan telah dilakukan melalui penghasilan prototaip berdaya maju minimum (MVP), mengikut rangka kerja Teknologi Pedagogi Kandungan Pengetahuan (TPACK) untuk pelantar e-pembelajaran. Empat orang ahli akademik berpengalaman telah mengesahkan Pengetahuan Pedagogi Kandungan (PCK) permainan dan dua orang ahli keselamatan siber profesional telah menguji Pengetahuan Teknologi Kandungan (TCK) permainan berkenaan. Kesan permainan telah diuji ke atas 71 orang pelajar universiti peringkat tertiari menggunakan reka bentuk kuasi-eksperimen dengan ujian pra-pasca kumpulan kawalan tidak setara. Kuasi-eksperimen ini telah berlangsung selama 24 minggu pada kohort ambilan pelajar yang berbeza dari dua buah universiti. Semua peserta telah menjalani ujian pra manakala kumpulan eksperimen bermain permainan SKRCTF secara berpandu. Selepas pendedahan kepada permainan selama 12 minggu, kumpulan eksperimen gagal menunjukkan perbezaan yang ketara dalam mengiktiraf ancaman keselamatan siber dan corak kriptografi. Dua puluh dua hipotesis nol telah disimpulkan untuk mengkaji kesan permainan SKRCTF ke atas pelajar yang baharu belajar memahami konsep keselamatan siber. Eksperimen kedua telah dijalankan selepas pelarasan panduan dan cabaran dalam permainan. Peserta menunjukkan sedikit peningkatan dalam pengiraan algoritma kriptografi asas dan mengenalpasti kod perosak mudah untuk akses tanpa kebenaran. Kesimpulannya, pemahaman pelajar tentang konsep asas sains komputer seperti sistem pengendalian, rangkaian, dan pengaturcaraan adalah penting sebelum menerokai pengetahuan keselamatan siber. Penyelidikan ini memberi implikasi berkaitan dengan kemahiran kognitif yang diperlukan sebelum menceburi keselamatan siber dan kesan latihan berasaskan permainan dalam mempelajari konsep keselamatan siber.

TABLE OF CONTENTS

CHAPTER 2 LITERATURE REVIEW

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Overview

This research synthesis an underlying model of utilizing a digital game framework as a tool for teaching cybersecurity in higher education. The game was developed based on the National Initiative for Cybersecurity Education (NICE) competency framework then validated by educators and industry professionals. This game instance can be adopted by secondary and tertiary educators, when using games to conduct skill-based teaching and learning activities of cybersecurity education. Validation from subject matter experts was obtained for the game toward the end of the research.

This thesis consists of six chapters. The first chapter provides an overview of the research, including the background, aims and objectives, research questions and hypotheses. The second chapter is a literature review covering the skill gaps and use of

Capture the Flag (CTF) in various security conferences. The third chapter reveals the research design and mythologies used in this study. The fourth chapter portrays the design, development, and validation of the CTF game. Chapter five reveals the findings after the hypotheses were tested. The final chapter concludes the research by explaining the significance and limitation of the research. This chapter briefly describes the research problem, research objectives, and key research questions, significance of the research and a short preview of each chapter.

1.2 Background of the Research

In advanced countries such as the United States, the National Initiative for Cybersecurity Education (NICE), under the National Institute of Standards and Technology (NIST), constructs a holistic framework to foster a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development (AlDaajeh, Saleh, et al., 2022). Without the support of an education framework for cybersecurity, Malaysian students are only exposed to formal Information Communication Technology (ICT) courses during their tertiary education. In the fast-evolving cybersecurity landscape, students will receive inconsistent knowledge and skills without a cybersecurity education framework. Compared to several countries implementing K12 education systems where cybersecurity concepts are introduced at the high school level (Borowczak, & Burrows, 2019; Page, Mekni, & Radday, 2023), Malaysian students require to speed up their learning in both ICT skills and specialized cybersecurity topics within their university term.

After the COVID pandemic, many organizations suffer a workforce gap in cybersecurity professions. Two established professional associations have produced survey reports that raised concern in this industry. Despite the multiple factors that lead to the spike in workforce demand, education reforms take years to witness the results (Rosenberg, & Starr 2020). Many security practitioners choose to attend workshops and security events to upskill and catch up with the quick ever-changing cybersecurity landscape (Chowdhury, Verma, & Mathur, 2020). The rise of CTF games for practicing cybersecurity skills is widespread in informal educational settings and as a highlight of cybersecurity conferences (Švábenský, et al., 2021).

The idea of conducting this research in nurturing cybersecurity talent in serious games was the result of the involvement in the review panel of Cybersecurity Malaysia's Global Accredited Cyber Education (ACE) Scheme and attending several established international cybersecurity conferences such as DEF CON, Hack in the Box (HITB), and Black Hat Briefings.

This study attempts to examine the effectiveness of a cybersecurity skill training game model through a quasi-experimental study on tertiary-level students in Malaysia. Participants' profiles will be depicted through a performance comparison between the pre-test and post-tests conducted to study the students' progression. The indispensable result from this research will contribute to the effort of enabling Malaysian technology students to build self-efficacy behavior in achieving a competency level in the dynamic cybersecurity landscape. The expected outcome of this study is to allow students to experience skill training through the fun yet frustrating problem-solving game.

1.3 Problem Statements

The US education sector has an immediate response after the President highlighted in his 2015 State of the Union message that building a highly capable cybersecurity workforce remains a top national priority (Karahan, Wu & Armistead, 2019). The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development to promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. The curriculum designs in NICE Cybersecurity Workforce Framework are aimed to increase the impact of cybersecurity educational practice in depth and breadth (Sherman, et al., 2020; Wetzel, 2021).

Reflecting the trend in Malaysia, in the effort of leveraging Internet Communication Technology (ICT) to scale up quality learning across Malaysia as part of Malaysia Education Blueprint 2013-2025 (Ministry of Education Malaysia, 2013), there is a huge gap to be filled in order to prepare Malaysian technology students to be as competence as a cybersecurity defender. The Malaysian Administrative Modernisation and Management Planning Unit (MAMPU) in 2015 embarked on the development of the Cyber Security Framework for Public Sector (Rangka Kerja Keselamatan Siber Sektor Awam, RAKKSSA). RAKKSSA is developed to guide the public sector in managing cybersecurity protection and government ICT assets. However, the framework focuses on maintaining the current IT implementations but

does not cover cybersecurity education in depth as a long-term solution to resist cybersecurity threats.

The challenge got tougher when Malaysia's world ranking in mathematics and science standards increased but fell below the middle point of scale in Trends in International Mathematics and Science Study (TIMSS) and Programme for International Student Assessment (PISA) 2018 (Avvisati, et al. 2019). Malaysian students scored 415 points (mean 487) for reading and 440 (mean 489) and 438 (mean 489) points for mathematics and science, respectively. This is a vital issue that cybersecurity topics cover not only covering programming logic but also computational thinking and troubleshooting skills.

Despite the investment flowing in with conferences and workshops to increase awareness, a constant upgrade in cybersecurity learners is needed to sustain the movement of defending against cyber threats. Emerging disciplines such as cybersecurity and data mining are not yet widely available at most higher education institutions (Yang et al., 2019).

The International Information System Security Certification Consortium (ISC)² estimates the size of the global cybersecurity workforce at 4.7 million people, with a workforce gap of 3.4 million in 2021 (ISC2, 2022). Asia Pacific region has the highest demand of a 2.1 million gap. 43% of the 12 thousand cybersecurity professionals mentioned that their organization was unable to find sufficiently qualified talent. This figure was supported by the ISACA professional body. In their State of Cybersecurity 2022, over 2 thousand security managers mentioned that their organization suffers from

unfilled technical cybersecurity professionals. This statement was supported by Wolff, who finds the scope of the cybersecurity landscape is vast and is distinctive from most of the profession that has uniform expectations (Wolff, 2021; Graham, & Lu, 2022). Educators find it challenging to reasonably standardize a core curriculum that students are expected to learn. Besides knowing organizational policies and operations, learners have a series of technical knowledge such as malware analysis, information protection, system security, network security, and others.

Personalized learning has shifted learning behavior. Learners used to be tested with replication of situations through multiple choice or short answers, but this phenomenon has gradually changed to virtual laboratories and online collaborations (Prendergast et al., 2023; Krüger Mariano, & Chiappe, 2021). However, utilization of the latest ICT facilities in Malaysia tertiary education is yet to be fully exerted especially in the sub-urban areas (Zainol et al., 2021; Rozmi, et al., 2019). The Common Teaching and Learning (T&L) process of cybersecurity courses is still following the conventional learning methods in tertiary-level education. Traditional approaches including lectures, coursework, live-through case studies, and paper-based case studies are often used to educate graduates. The T&L process should stimulate the learner's intrinsic motivation to explore the lesson that has been taught (Chaudhuri, 2020; Zang, et al. 2022). This is because learners still prefer to refer to the lecture notes during their post-learning session to understand the theories, thus being able to link the theory with the actual application. In other words, learners must imagine within their minds just to be able to combine the concepts and theories learned without a clear learning medium during assessments. Despite having different student learning capabilities, to prove

their efficiency, this research will also provide empirical evidence to support the use of CTF towards the T&L of cybersecurity.

There is a need to increase the interest of the future Malaysian workforce in defending against cyber threats, covering from home to organizational environment. Influenced by the increment of cybersecurity awareness but constrained by the gap in ICT skills between Malaysian students and other countries, this research aimed to design, develop, and validate a game model for cybersecurity education using CTF before moving into a higher level of challenges.

1.4 Research Aim and Objectives

This research aims to validate a framework of game-based cybersecurity teaching and learning. Efficiency in obtaining cybersecurity skills within a limited time becomes an important matter. Undergraduate degree students have an average of four years of studies to acquire knowledge and skills in cybersecurity, before entering the workforce associated with cyber and information technology (IT). The summarized problems identified in Section 1.3 were:

i. Malaysia lacks a framework for T&L cybersecurity.
ii. Malaysian students suffer a skill gap in the cyber security area in global competitions.
iii. There is no guideline for Malaysian educators in delivering cybersecurity modules.

A CTF game has been recognized as the game to support this T&L framework. This game is embedded with real-time gameplay, which possesses generic game characteristics, such as an avatar, scoring system, instant feedback, social connections, and reward, affording lecturers or instructors to monitor learning progress. The game can capture real-time data for use in analyzing a framework for T&L cybersecurity. To attain the research aim, the following research objectives are formulated in this study:

i. To design, develop and validate a CTF game for teaching cybersecurity among undergraduate students.
ii. To compare the differences in undergraduate students' knowledge acquisition on fundamental concepts in cyber security before and after learning through a CTF game.
iii. To validate the differences in undergraduate students' knowledge acquisition on types of threats in cybersecurity before and after learning through a CTF game.
iv. To validate the differences in undergraduate students' knowledge acquisition on cryptography in cybersecurity before and after learning through a CTF game.

The T&L framework is based on a constructive mapping of the Introduction to Security module in Bachelor of Science Year 1. An initial prototype will be tested and evaluated by lecturers and subject matter experts. Pilot test evaluation with students and assessor will be followed up.

1.5 Research Questions and Hypothesis

The main research question for the study is: How can a framework for T&L cybersecurity using CTF help tertiary-level students and lecturers? More specifically, the research questions that can be generated from the objectives are:

i. How to design, develop and validate a digital game of CTF using Huang and Soman's 5-step gamification for teaching cybersecurity among undergraduate students? (*Objective 1*)
ii. Is there a statistically significant difference in students' performance in acquiring fundamental cybersecurity concepts before and after learning through a CTF game? (*Objective 2)*
iii. Is there a statistically significant difference in students' performance in acquiring types of cybersecurity threats before and after learning through a CTF game? (*Objective 3*)
iv. Is there a statistically significant difference in students' performance in acquiring cryptography concepts before and after learning through a CTF game? (*Objective 4*)

Begin with the end in mind, students need to be equipped with cybersecurity skills and knowledge upon graduating. Hence, the null hypothesis to test the efficiency of learning cybersecurity knowledge and skill in this research is:

i. H_0: There was no significant difference between the total pre-test scores and total post-test scores of the control group and the experimental group.

ii. H_1: There was a significant difference between the total pre-test scores and total post-test scores of the control group and the experimental group.

iii. H_0: There was no significant difference between the pre-test scores and post-test scores of the experimental group in recognizing cybersecurity threats.

iv. H_1: There was a significant difference between the pre-test scores and post-test scores of the experimental group in recognizing cybersecurity threats.

v. H_0: There was no significant difference between the pre-test scores and post-test scores of the experimental group in recognizing cryptography patterns.

vi. H_1: There was a significant difference between the pre-test scores and post-test scores of the experimental group in recognizing cryptography patterns.

1.6 Conceptual Framework

The focus of this study was undertaken by the following conceptual framework shown in Figure 1.1. Figure 1.1 shows the conceptual framework of SKRCTF Game in a high-level view. The game consists of multiple challenges but revolve within two main topics of cybersecurity threats and cryptography patterns. Learners are split into two groups, and they are taking the same pre-test. one of the groups is exposed to SKRCTF game. Both the groups are taking the same post-test to examine if the exposure of SKRCTF game provides significant difference in the learning cybersecurity skill. The exposure of SKRCTF was the independent variable in this experiment, while the learner's pre-test and post-test scores were the dependent variable. The significant differences in the post-test scores could change depends on the depth level of exposure among the treatment group to the game.

Next, the mapping of the Technology, Pedagogy and Content Knowledge (TPACK) model on SKRCTF game is included into the framework. The SKRCTF game development and validation process from the collaboration between educator and CTF creator in the effort of creating the CTF and challenges for the learners.

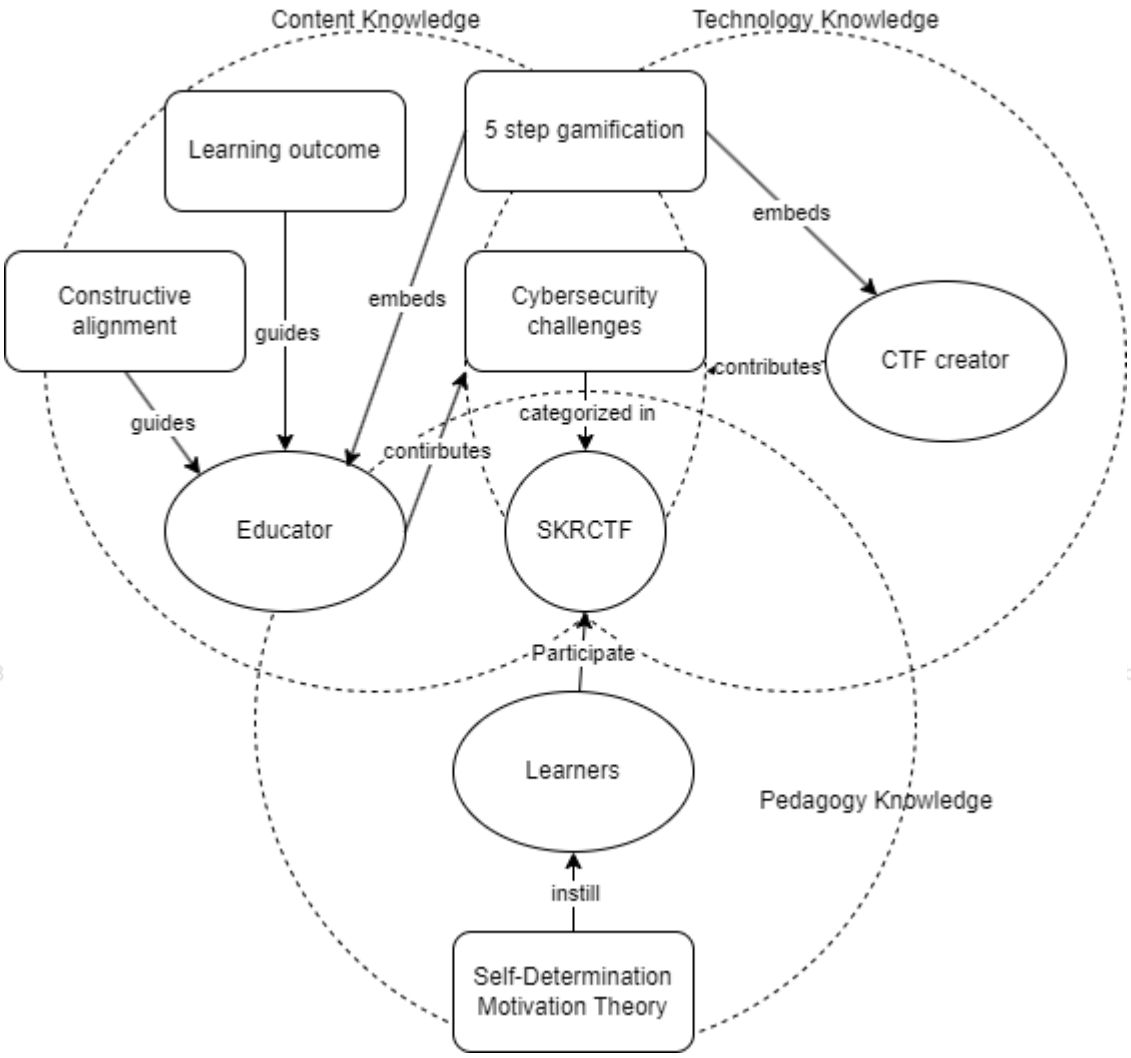
The educators will obtain the learning outcomes from the qualification bodies. Similar to offline teaching methods, a constructive alignment was conducted to map the learning outcomes to the current semester curriculum content. Then, the educator will select the best fit topics related to cybersecurity threats and cryptography to collaborate with CTF creator to create the challenges into SKRCTF. The learner's performance will be reflected in the CTF scoring system and the educators can evaluate their performance and challenges faced.

CTF creator on the other hand is playing a supporting role to the educators. The CTF creator will build and maintain the CTF infrastructure such as scoring system and game availability. The CTF creator does not accompany the educators and learners for the period of study but only occasionally where IT technical support is required.

SKRCTF will be the centered focus of the TPACK model where technology, pedagogy and content knowledge are the three constructs integrated to validate the successfulness of the game for learning. Both the educator and CTF creator are expected to equip with Huang and Soman's Five-step gamification (2013), the steps cover: i) understanding the target audience and the context; ii) defining learning objectives; iii) structuring the experience; iv) identifying resources; v) applying gamification elements.

Figure 1.1

The Conceptual Framework of TPACK for SKRCTF



1.7 Significance of this Study

Game-based Learning (GBL) is not new in the education sector (Tan, 2012; Garcia, et al. 2020). This research is to extend GBL to develop typical profiles for specialized track students in Malaysia, especially in the cybersecurity field. The study outcome will

be redounded to cybersecurity education. Educators will be guided on what should be emphasized in the curriculum. Learners who apply the learning approach will not only acquire cybersecurity skills and knowledge but also develop employability skills. Focus on developing cybersecurity games will not be generating any impact as there is already some literature on games for Science, Technology, Engineering, and Mathematics (STEM) education focusing on cybersecurity (Scholefield & Shepherd, 2019).

This research is targeting Malaysian cybersecurity students to be self-sustaining in adapting to the dynamic cyber threat landscape. The roadmap of a cybersecurity practitioner starts from the front line such as security testers and incident responders before evolving to a managerial role such as department leaders and policy makers. This research is aimed to extend GBL to a specially focused industry operating on a diverse platform that requires logical reasoning and operations. The study will be supported by creating and assessing the logical-mathematical intelligence from the seven core intelligence profiles of Gardner (Wiliński, & Kupracz, 2020; Gardner, 2011). This research will also empower educators to focus on T&L process and assessments in helping students to achieve the industry needs.

1.8 Research Scope and Limitations

The scope of this study extends the use of technology-enabled innovations to deliver and tailor education for students. It is important to study the motivation factor of students finding digital games to aid them in obtaining the skills and knowledge.

The discussion of Capture the Flag (CTF) for cybersecurity could replace formal education is legitimate but is not the context of this research. Studies found that there are gaps between novice and advanced learners in learning both science and arts subjects (Stein, Gurevich, & Gorev, 2020; Suzuki, Nakata, & Rogers, 2023). Therefore, this research is aimed to extend gamification in learning fast-evolving cybersecurity topics instead of making gamification the main education framework.

Extending the framework in gamification for focused groups such as cybersecurity might cover a limited education context with limited cybersecurity programs offered in Malaysian tertiary-level education. An expected 60 participants fitted the quantitative data analysis at the time of this research but are considered relatively small.

In some restricted situations where the educator is the CTF creator, additional resources are needed to meet TPACK model requirements, as shown in Figure 1.1. The educator may require more resources in handling content development, game design and development, and game testing.

a) The Participants

University students are the direct target to experience the impact of this research. They are at the stage of exposing themselves to the industry. Primary and secondary students are too young to appreciate the need to master cybersecurity. Despite the age group and intellectual gap, the cyber landscape is changing drastically (Cheng, & Wang, 2022) which heavily influences the cybersecurity trend. Educators are the direct communication personnel to students in universities. Their contribution to molding

students' knowledge, skills, and ability is vital. Educators will contribute secondary data for the experience of using CTF games in delivering cybersecurity content. Subject matter experts in various industries are included in the design phase. They are called upon to provide expert validation of the CTF game and the pedagogy of T&L cybersecurity.

b) The Game

CTF is developed with the core instrument in challenge creation, flag submission, and score calculation. Score integrity is the focus of the game as real-time feedback occurs during the gameplay. The player's score reflects the motivation factor to retain and benefit more from the game. Physical internetworking devices aside, the source code of the game must be reviewed to prevent intentional and unintentional in-game threats. On the other side, the assessor can obtain real-time data from the game by checking submitted answer verifications, challenge creation, and real-time game monitoring. Hence, the word "Game" is used instead of "Platform" in this research. CTF game is run under an isolated environment. This is to avoid any disruptive threats from spreading to the public. The game code will be installed in the main server and participants are connected to the game for challenges retrieval and submission.

c) The CTF Game

CTF is conducted for a limited time in rounds, unlike a generic digital game. It has a similar nature to physical sports games where participants are given limited time to complete a series of tasks. CTF participants are assigned to search for the answer key string from various digital evidence and submit it into the scoring system. Winners are determined by the fastest and the most correct answers.

A CTF named Script Kiddie Resilience Capture the Flag, SKRCTF is customized for this research. It will be a twelve-week CTF session with one hour per session to be conducted in two local private universities that offer cybersecurity Degree programs. The course mapping and CTF details are listed in the appendix.

Five steps gamification process is used in designing SKRCTF (Huang & Soman, 2013, Ardiana, & Loekito, 2020). The steps are: 1) Understanding the target audience and the context; 2) Defining Learning Objectives; 3) Structuring the Experience; 4) Finding Resources and 5) Applying Gamification Elements. Figure 1.1 shows the SKRCTF creator embedded the five steps gamification during the game design and development of the CTF game. The game design process is not affected by the twelve-week duration, unlike the usual CTFs that run between 24 to 72 hours.

1.9 Operational Definitions

This section provides clear explanations of terms and concepts used in this study. This is to align the readers to achieve mutual understanding and interpret key terms in the same way.

a) Teaching and Learning (T&L) Framework

The T&L framework is a set of guidelines designed to support teachers in the subject delivery which aim to improve students' ability to learn and understand the subject being taught. An underlying structure where something can be built. It also acts as a system of rules, ideas, or practice relating to effective ways that empower students in

learning. In cybersecurity, the learning activities require a learner's skill and knowledge especially on the operational competencies needed by a cybersecurity professional. Hence, this research uses the personalized, Game-Based Learning approach through Huang and Soman's five step gamification.

b) Cybersecurity

Cybersecurity is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage, or unauthorized access. In a computing context, security includes both cybersecurity and physical security. Following the National Initiative for Cybersecurity Education (NICE) framework, fresh graduates usually start with a junior position that relies heavily on technical skills, that is recognizing and tackling cybersecurity threats. Other domains such as governance, policies and provisioning require cumulation of work experience. Hence, this research will only cover the topics of cybersecurity threats and cryptography, exclusively on web exploitation, malware, and weak cryptography algorithms.

c) Capture the Flag (CTF)

A game in which players on each of two teams seek to capture the other team's flag hidden in each other's base camp. In a digital CTF, players on each team try to obtain the puzzle key from the challenge server. Winners are determined by the most correctly submitted flag in the shortest time. A customized CTF known as SKRCTF was designed, developed, and validated for this research purpose. It covers a scoring system, challenge creation, team and user management, and anti-plagiarism mechanism. This research will be focusing on challenge creation and guidance such as hint and write up.

d) Intrinsic Motivation

Learners perform a task without any persuasion or instructions as they enjoy the task as an opportunity to explore, learn and actualize their potential. 4 motivational theories were derived from a variety of motivation research to suit the SKRCTF. The theories are: i) Self Determination (SDT); ii) Goal Setting Theory; iii) Flow Theory; iv) Expectancy-Value Theory. This research adopts the most common SDT that fit most criteria of SKRCTF especially on learner's competency, autonomy, and staying connected. The motivation theory applies while the CTF creator is converting challenges to fit into SKRCTF. Detailed reviews were conducted in section 2.4.2.5.

e) Score

The measurement of score in this research is using a nonparametric test that measures the consistent differences between the control and treatment groups' post-test score. The difference in medians is further assessed with Wilcoxon signed-rank-test where the location of the probability distribution of the pre-test and post-test within the same study group.

In the usability test, Software Usability Measurement Inventory (SUMI) is used to measure the software quality from the end user point of view. It uses a likert scale with three categories: Agree, Don't Know, and Disagree. The score within one standard deviation of the mean is measured between 40 and 60, which the software will be defined as above or below the average of 50.

f) Learning Objectives

Learning objectives (LOs) are specific statements that define the areas students are expected to learn. Each subject at different levels of study has set different LOs to specify the teaching and learning that take place, with specific directions and expectations on the activities to achieve the goals.

LOs are common in both conventional teaching and GBL. There are on average three to five LOs per subject. Skill based training especially in cybersecurity CTFs requires specific competencies especially psychomotor and cognitive skill as foundation. In SKRCTF, three pillars of the Technological Pedagogical Content Knowledge (TPACK) framework are defined in chapter 2.

g) Technology Knowledge (TK)

This domain in the TPACK framework requires the understanding of specific technologies involved in creating and deploying games. CTF is different from conventional 2-Dimensional and 3-Dimensional games. The game platform creator needs to equip the knowledge of web development, databases, and cybersecurity software. Learners are guided to identify and utilize various cybersecurity tools, evaluating different technologies to aid them in tackling the given challenges.

h) Pedagogy Knowledge (PK)

This domain requires both educators and game creators to design the game in a way that promotes active learning, critical thinking, and problem-solving. Designing CTF challenges will incorporate formative assessments to guide students through different stages, embed hints and support, and facilitate collaborative learning through

discussions. Engaging in active learning for skill training has its challenges. Practices and reinforcements are constantly needed throughout the CTF sessions. Learners are encouraged to apply problem-solving skills and perform constant self-reflections.

i) Content Knowledge (CK)

Cybersecurity landscape is dynamic but the complexity lays on several core concepts. Deep knowledge of cybersecurity concepts that need to be delivered to the learners. Educators themselves would need to catch up with several cyber threat kill chains and methodologies before recreating them into the CTF environment. Learners will be benefited from the challenges by analyzing and solving the challenges while applying the theories into practices.

j) Game Mechanics

CTFs is different from any 2-Dimensional and 3-Dimensional computer games. Participants are given a set of IT challenges and required to obtain a piece of valuable information from the challenge as the flag. There is more than one approach to obtain the flag. Hence, the game mechanics such as challenges, and scenarios are designed to align with the learning outcomes and suit the participants' behavior when participating in a CTF session.

k) Cybersecurity Threats

Threats occur when there are risks and vulnerabilities. Applications and systems are developed in different codes, languages, and platforms. Vulnerabilities can be found in many aspects and they can affect other components of the applications. Learners are exposed to various codes and applications, paced with different complexity levels to

exploit the vulnerabilities. They are taught to simulate the exploitation or defend the challenge by patching the vulnerabilities.

l) Cryptography Patterns

Cryptography is the common introductory module to be taught in cybersecurity courses. It emphasizes the practice and study of techniques for securing communication and data through encoding information so that only authorized parties can access it. It involves mathematical formulas in converting the texts to codes and vice versa.

Learners are trained to recognize various encoding methods in the proposed CTF. Principles and applications of cryptography, such as encryption, decryption, and key management are taught and assessed. Learners are guided to recognize if the encryption was used in various situations.

1.10 Summary

The chapter begins with an overview of the research topic, emphasizing the importance of cybersecurity education in the current digital age and the innovative approach of using CTF games for skill development among novices. This research delves into the current landscape of cybersecurity training, highlighting the gaps in traditional educational methods. It discusses the increasing need for practical, hands-on training to equip undergraduates with the skills to recognize and mitigate cybersecurity threats. The problem statements identify the specific challenges and deficiencies in the current cybersecurity industry and education. These include the lack of engaging, practical

training methods and the difficulty in keeping training programs up-to-date with the rapidly evolving threat landscape. These issues are substantiated with references to studies and statements from cybersecurity professional bodies such as ISC2 and ISACA. These statements led to the aim of the study: to develop an effective, skill-based training program using CTF games. The objectives include enhancing students' abilities to identify cybersecurity threats and recognize cryptographic patterns through interactive and gamified learning experiences. Key research questions that guide the study, such as "How to design, develop and validate a digital game of CTF using Huang and Soman's 5-step gamification for teaching cybersecurity among undergraduate students?" and "Is there a statistically significant difference in students' performance in acquiring fundamental cybersecurity concepts before and after learning through a CTF game?". Hypotheses are formulated based on these questions, providing a foundation for the research methodology. A conceptual framework is introduced to illustrate the theoretical underpinnings of the study. It maps out the relationship between SKRCTF, educators, CTF creators and learners. The framework also adopted the use of the TPACK framework serving as an underlying guide for the research design and analysis. The scope of the research is defined, focusing on undergraduate students and the specific areas of cybersecurity threats and cryptography. Limitations are acknowledged, such as the potential variability in students' prior knowledge and the challenges of measuring skill improvement objectively. This chapter ends with key terms and concepts used throughout the research are clearly defined to ensure consistency and clarity. This includes definitions of game-based learning, cybersecurity threats, cryptography patterns, and the structure and purpose of CTF games.