Tallinn University of Technology
School of Information Technology

Maria Lourdes Bacud IVGM 1942 92

Designing a Users' Experience Model using Game-Based Learning as Capacity Building Approach in Cybersecurity Awareness for the Public Sector

Master's Thesis

Supervisor: Sten Mäses

PhD, Cybersecurity

Tallinn
2021

Tallinna Tehnikaülikool
Infotehnoloogia teaduskond

Maria Lourdes Bacud IVGM 1942 92

Kasutajakogemuse Disainimine Mängupõhise Õppe Abil Turvateadlikkuse Kasvatamise Võimekuse Suurendamiseks Avalikus Sektoris

Teadusuuringute ettepanek

Supervisor: Sten Mäses

PhD, Cybersecurity

Tallinn
2021

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis and this thesis has not been presented for examination or submitted for defence anywhere else. All used materials, references to the literature and work of others have been cited.

Author: Maria Lourdes Bangug Bacud
10.05.2021

Acknowledgement

Time is of the essence.

I always better myself in every possible way I could because it is one of the limited ways to help my country, the Philippines. We were among those students funded by the state to study in the premier state Universities in the country to acquire the best possible education (Iskolar ng bayan). That well-protected nationalism and patriotism are instilled up to our core (#parasabayan).

But COVID-19 happened. It allowed us to reframe our priorities, our families. It came clear to me that I am doing my best to excel to offer the best conceivable opportunities for my family because *time is of the essence*. But pandemic took and is still taking away important time with them or worse, taking them away from us perpetually.

I wholeheartedly dedicate the fruits of sleepless and eureka days and nights to my *Mama* whom we have lost because of the COVID-19. She made me a capable and reliable being before the world ever knew I could. I share this knowledge to my bereaved family (*Papa, Kuya/ elder brother, and Aunt beth*), who were also victims of the unforgiving onslaught of the virus. They made sure Mama received every possible treatment and care while I am here writing this paper.

To my friends around the world who made sure I am surrounded by prayers, and sincere love and care as I struggled to put myself together, tightest hugs. I am forever grateful to the frontliners of this war who have painstakingly and tirelessly keeping us safe while they set their lives and family at risk.

The guidance and patience of my supervisor, Stan Mäses, is sincerely appreciated and treasured. Thank you for choosing me. Thank you for letting me to be me in this academic paper.

And above all, to God be the glory.

It might not be now or not even soonest, but in His time, everything will make sense.

Abstract

Public sectors’ capacity to use electronic systems should move parallel with the awareness and ability to protect these systems and data captured. This paper seeks to contribute to the optimization and strengthening of cybersecurity awareness initiatives. Primarily, it identifies an effective and sustainable learning experience by designing a users’ experience of a cybersecurity awareness training for public sector using game-based learning. Reinforcing the learning content with innovative learning experience and digital technologies, to wit, serious games can make learning more effective and engaging. This study provides an evaluation of online serious games used tackling cybersecurity awareness and analysis of the motivational core drives using the Octalysis framework. While the Octalysis gamification framework is widely used in the design of serious games, it is still rarely implemented to tackle cybersecurity challenges. This paper demonstrates how cybersecurity awareness trainings are closely connected to motivational factors and how a systematic approach, such as Octalysis framework, can help to compare the various aspects of different awareness programmes.

This paper also provides analysis from the key informant interviews from experts and implementors of cybersecurity awareness programmes, and serious games on the key considerations to integrate the cybersecurity awareness initiatives and game-based learning to improve learning outcomes. Finally, the study presents a users’ experience design that may contribute to the optimization of learning and sustaining learning experience in cybersecurity awareness with game-based approach.

Keywords: Cybersecurity awareness, Game-based Learning, Serious Games, Octalysis, Simulations for e-Learning, Public Sector Capacity Building

This thesis is written in English contains 78 pages, 6 chapters, 8 figures, and 5 tables.

List of abbreviations and terms

CCDCOE	Cooperative Cyber Defence Centre of Excellence
CSIS	Center for Strategic and International Studies
EC	European Commission
ENISA	European Union Agency for Cybersecurity
EU	European Union
FGD	Focus Group Discussion
GBL	Game-based Learning
GDPR	General Data Protection Regulation
G2E	Government to Employees
ICT	Information and Communication Technology
KII	Key Informant Interview
MGIEP	Mahatma Gandhi Institute of Education for Peace and Sustainable Development
NCSI	National Cyber Security Index
NGO	Non-Government Organization
RIA	Riigi Infosüsteemi Amet (Information System Authority)
UNESCO	United Nations Educational, Scientific and Cultural Organization

List of Figures

List of Tables

Table of Contents

1 Introduction

1.1 Overview of the study

Cybersecurity is deemed as an essential part of digital society [1]. It is accepted universally as an important part of the function of the state, economy, and internal and external security [2]. This was fully realized in European Union after the “cyberattacks against Estonia in 2007” of which called for a “cyber awakening” [3]. The inception of countless cybersecurity documents emerged in European Union, such as, GDPR, Cybersecurity Act, Network and Information Security Directive, etc. In a brief definition provided by the Cybersecurity Act of 2019 (Article 2), “cybersecurity pertains to the activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber hazards” [4].

The mandate to enforce and protect cybersecurity are in place, however, these are yet to be assessed on its effectiveness and appropriateness in the fast-changing world of digital space. Cybersecurity has interdependencies which makes privacy and security by design challenging [3]. It entails not only the actual system but also includes the entire network of resources and functions from technology to human behaviour. As we expand digitisation and connectivity, cybersecurity risk intensifies inducing the vulnerable society to another level of threats [4] which leads to unimaginable impact to the interwoven functions and lives of social fabrics.

The current circumstance created by the COVID-19 pandemic has heightened the urgency to shift operations and functions typically done on-site moved to on-line. This seemingly workable set-up opens another space of vulnerability from controllable networks to expanded insecure systems. The cyber risk intensified by newly adopted work environment posed a more complex and challenging digital space management. The unimaginable speed of development of technologies like 5G, and internet of things (IoT) is another layer of complexities [5] which in some cases may ease up, but often, prolong uncertainties. INTERPOL Secretary General Jürgen Stock highlighted, “Cybercriminals heightened cyberattacks development at an alarming pace amidst the COVID-19, exploiting the fear and uncertainty of insecure social and economic crisis pandemic has created” [6].

As Estonia accelerates its capacity on cybersecurity, appropriate platforms, and systems to support this enterprise are being expanded to date. Platforms and systems are not only being updated or strengthened; the knowledge and skills of the human resource are moving in parallel. Capacity Building namely awareness and training are perceived as effective approaches in managing threats and impacts of compromised cybersecurity integrity [7]. Various learning approaches have been utilized to ensure the achievement of the targeted capacity development.

Estonia ranks 3rd in NCSI to date [8]. Known for its 99% online government services [9], it released its 2019- 2022 Cyber Security Strategy. The document explicitly identifies four (4) strategic objectives to develop/ strengthen its digital society. Objective 4 indicates a "cyber-literate society" by raising cybersecurity awareness among citizens, state, and private sector from its status quo- low cybersecurity awareness [2]. For an advanced digital state like Estonia, a cyber-literate society is a foundational strategy to strengthen key areas of the country's affairs.

Game-based learning methods are recently being adopted to cybersecurity training while fields of healthcare, advertising, and behavioural change utilized this platform long before [10]. As it evolves as a viable process and practice for learning, custom-built game targeting a specific objective or Serious Games emerges as powerful game-based initiative which focuses more beyond its primary purpose of entertainment [11]. Game-based learning itself is not a full guarantee to sustain the use and participation of users in a dynamic profile of an organization. Learning how to strategically position motivational enhancement tools (game elements) would drastically change the landscape of capacity building.

For capacity building, game-based learning is relatively new-found concept for cybersecurity awareness and only known few games focus on adult population [7]. Efforts driven to build cybersecurity awareness to community is as important as strengthening the public sectors' (government) capacity in dealing with cybersecurity threats. In most organizations, if not all, the topic of cybersecurity awareness is the initial touch point to educate employees on various fields. A lot of adult- learning strategies were used in the past and still being utilized at present. A different approach could optimize processes and results which every society deemed necessary. Learning from a cybersecurity awareness training can only be effective if done in a safe environment where repetitive failure is seen as input for learning optimization. A simulated environment for practice can facilitate the transfer of learned theories to practice. Reinforcing the learning content with innovative learning experience and digital technologies such as serious games can make learning more effective and engaging.

Furthering research on this matter would contribute to the body of knowledge gearing to Game-based learning as potential option to support key areas of cybersecurity capacity building initiatives. It also seeks to form part of the limited body of knowledge on the government to employee (GTE) research, design, and use of digital and innovative solutions for the human resource management of the public sector. Moreover, this intends to contribute to the strategic objective of Estonia on a cyber-literate society.

1.2 Thesis motivation

Digital by default is the new norm. The COVID-19 pandemic triggered the unimaginable acceleration of the digital transformation on ways things are being done from providing public services to digital presence in a global forum or mere attendance to a family reunion. The world had that needed pause for quite strides to make the shift, effective at the very least, to a working space only few have amassed months back. Cyberspace is deemed to be the only option otherwise a total shutdown which would never be a convenient route for everyone. While all are in the run for appropriate and within means digital tools and systems, security by default principle is hanging by the ledge yet to be unravelled only after the would-be ramifications of a system breach. This is how most are perceiving cybersecurity, an afterthought.

The surge of unrestricted and insecure networks weakens the thriving efforts to calm the uncertainties. This creates upfront worries and ambiguities on which among several options to support the work from home set-up could optimize results. These known and surfacing vulnerabilities are enough loopholes for those who want to take advantage of the unstable systems. Organizations respond to threats and ensure a cybersecure digital space by making systems smarter and robust enough to uphold its functions. The human resource, the most vulnerable in the spectrum, yet an important aspect in building cybersecurity has to be aligned with the speed and innovations in place for the highly valued information assets. Human resource capacity to support the cybersecurity initiatives should never be an afterthought.

Efforts driven to build awareness to community is as important as strengthening the public sectors' (government) capacity in dealing cybersecurity threats. Public sectors' capacity to use electronic systems should move parallel with the awareness and ability to protect these. Awareness is the initial touch point to educate human resource on a certain field. Being at the forefront of the initiatives on learning, awareness should be as effective as of those strategies for in-depth learning for complete mastery. Learning from a cybersecurity awareness training can only be effective if done in an almost actual scenario [12]. A simulated environment for practice can bridge the learned theories to practice. Reinforcing the learning content with innovative learning experience and digital technologies like Games can make learning more effective and engaging. This aspect of eGovernance is as relevant as its usual facade of technologies and strategies.

The human aspect or the G2E aspect in the eGovernance is always the core of discipline of the author of this study. Identifying the appropriate technologies and developing its seamless functions do not end on its own. eGovernance allows the optimization of the government services and information to citizens with the use of technology and innovations while ensuring the acceptance of its target users and beneficiaries to adopt these services [13]. Acceptance entails various methods of which is capacity building. It is an approach to sustainably integrate while empowering the users and beneficiaries of the e-services. Study on viable options to ensure effectiveness and efficiency of capacity building initiatives on eGovernance, in this case, *cybersecurity*, is the chosen track of endeavour of the author of this research.

1.3 Research Questions

The study investigates conceptually and empirically the Users' Learning Experience using Game-based learning as capacity building platform in cybersecurity awareness for public sectors in Estonia. To put this into context and guide the process of the research, questions are formulated, to wit:

RQ 1: How do online games for cybersecurity awareness position its core motivational drivers?

Games for cybersecurity awareness specifically for adults are systematically searched and assessed. The results of the assessment will present an overview on the game design used and prioritized in the entire journey by identifying the core motivational drivers in place vis-à-vis user/ gamer journey phase. It will be an inventory of cybersecurity awareness games and motivational drivers' profile of each game.

RQ 2: How can game-based learning be integrated into the cybersecurity awareness capacity building approach for the public sector?

Considering a shift on the learning environment to another platform will always have various key concerns for a seamless integration of the proposed platform. Key informant interviews with the various experts and implementers in the fields of cybersecurity, and game-based learning are specifically targeted to shed light on the harmonious collaboration and anticipated challenges in the merge.

RQ 3: How can game-based learning improve learning and learning experience in the cybersecurity awareness training?

To influence and propose for a design of the learning experience, the study seeks the users'/ learners preferred experience that could optimize learning and sustain the learning experience. Users/ learners of the cybersecurity awareness training in the public sector of Estonia are targeted to participate in a FGD facilitated by the author of the study. The result of the methodology will present preferred game design elements and motivational traits in place to reinforce learning and support learning process.

Results of the study would like to support the activity area 4.1 of the Estonia's Cybersecurity agenda 2019- 2022 on raising cyber awareness for the workforce of the state. Findings may be found relevant input on the planned common/ nationwide platform for cybersecurity literacy. This may expand the viable options of platform or strategy in ensuring learning outcomes for government workforce in raising cybersecurity awareness. This will also contribute to strengthening the knowledge and skills of government frontliners and middle-managers. Results of the study may also influence how various eGovernance institutions design and conduct training to its local and international public sector workforce.

Certainly, the study would like to contribute on the strengthening of the capacity building of the human workforce providing e-governance services. An *informed* and *well- equipped* government workforce supports the seamless delivery of public services, including data privacy and protection. The development of state-of-the art systems/ software does not end on its own. People bound to implement this should embody the intricacy of the product. We are not only creating smart system solutions; we create smarter and stronger human resource.

1.4 Thesis Outline

The thesis is organized in six (6) important chapters to substantiate the process from inception to results which will be contextualized comprehensively to respond to the research questions. Chapter 1 introduces the thesis goals and underscores the identified problem to be solved. Chapter 2 provides literature and theoretical constructs of which study is based on. It also elaborates the past studies on Octalysis and its practical application in various fields apart from cybersecurity.

Chapter 3 expounds the systematic processes involve from data gathering to the analysis of the results. Underlying reasons on how the study arrive to a certain circumstance are specifically indicated in this section. The present study will utilize qualitative research method.

Chapter 4 elaborates the result of the conceptual and empirical inquiry done. This section will include the captured data from various data gathering tools used such as systematic games search, key informant interview, focus group discussion. The results from KII and FGD will be analyse systematically utilizing thematic analysis. More importantly, it provides a more in-depth discussion and making sense of the data gathered from various tools. Discourse on the results will form part in the proposed design of the users' learning experience model. The results of the study would be beneficial to gaming industry to improve game design, organization (public sector) considering game-based learning as platform for cybersecurity awareness, and project management designing a targeted learning experience for cybersecurity using game-based learning

Chapter 5 presents the limitation and the proposed way forward for the study (implementation or further study).

Chapter 6 summarizes the research process, and key findings of the thesis.

2 Theoretical Background

2.1 Digital Transformation and Cybersecurity

Digital transformation is deemed the most impactful initiative evident on the way various organizations change its way of doing things and interacting with its stakeholders. While being the most impactful, cybersecurity aspect of the digitalization is considerably the biggest and serious challenge posed by these changes [14]. The current circumstance COVID-19 has created another layer of challenge [15]. International Criminal Police Organization (INTERPOL) released a report showing the impact of COVID-19 on the shift of cybercrime target from attacks involving individuals/ small-scall businesses to larger and major private organizations, governments, and important infrastructures.

From January-April 2020, significant number of attacks were captured all related to COVID-19 consisting of “more than 900,000 recorded spam mails, malware associated incidents, and 48,000 linked with URLs that are suspicious looking” [6]. These have yet to be translated to economic losses which is expected to exceed the previous year’s reports. Australia calculated a “surge to $1 billion direct cost every year” as reported by Australian Criminal Intelligence Commission cited in the study of Chang and Coppel in Building cybersecurity awareness [16]. Cyentia Iris 20/20 reported an average of $47M for extreme cyber events in early 2020 [17].

The significant surge of attacks can be attributed to the rapid shift to remote systems and networks allowing a functioning operation of organizations which supports the economy [15]. Criminals recognize the vulnerability from this shift; thus, this is being taken advantage to take hold of various data in exchange for money and provoke process disruption. This imposed relevant cybersecurity measures. But security assurance remains a challenging task [18]. The appropriateness of measures to the circumstance of every organization varies- not a one-size fits all strategy.

According to a study conducted in 2010, websites of public sectors have limited measures in place to ensure security [19]. This may be attributed on how an organization values cybersecurity and measures that come along with it. While having limited protective measures in place, government administration remains as viable target sector [20] and on the top list that experience attempts of damaging attacks [21].

This aspect of information society needs critical planning concurrently as every state defines concrete ways forward in transforming its services and eventually the entirety on how the society works. With the constant and unimaginable increase in number and occurrences of cyberattacks curated to take benefit of the unsuspecting organizational employee, the significance of the human aspect in managing information security cannot be downplayed [22]. World in the middle of pandemic is gearing up now, more than ever, to digital transformation. Everyone is in the hunt to create an appropriate platform to digitize services and an effective ecosystem for seamless interoperability and uninterrupted provision of services. While everyone is planning to shift on digital platform, it is equally important more than ever to further the capacity of everyone on cybersecurity.

ENISA recognized the unrelenting complexities of cybersecurity risk advancement in the next decade. Assessment and interpretation will become challenging more than ever as the threat landscapes and amplification of the attack domains develop their intricacies [23]. In ENISA's report published in October 2020 (reports captured from early 2019 – 1st quarter of 2020), the following are the top 10 threats in this order, "Malware; Web-based attacks; Phishing; Web Application attacks; Spam; DDoS; Identity theft; Data breach; Insider threat; Botnets" [24]. These were initiated by humans fuelled with human motivations [25] which mostly driven by financial gain [26].

According to the Cybersecurity Act, EU defines cyber risks and hazards as "any potential incident, event or action that could harm, interrupt or otherwise adversely impact network infrastructure and information systems, the users of these systems and other persons" [4]. Impact may vary depending on the system/ data prone to attack vis-à-vis its criticality/ dependencies to the organization which eventually create ripple effect to other operational areas. The extent of the impact varies on the measures taken to respond identified cybersecurity risks before it can be an actual attack.

In a CSIS 2020 report, monetary loss incurred by cybercrime surged at nearly $945 billion while global pay out in cybersecurity will exceed to $145 billion [27]. The same report approximated "$1 trillion set-back on the global economy" in 2020 and a projection of increase in the coming years. However, most of the impact of the cyberattack was not calculated into specific cost, missed opportunities, emotional distress of employees, reduced efficiency, loss of trust [27] and (worse) disruption in the lives of many most especially those in the peripheries of poverty who are highly dependent to government support.

Certainly, organizations and regional associations intend to cut cyberattack impact. Strategic plans and measures are being agreed on to take effect. Many have seen the need to further cyber threat intelligence capabilities and training which remains limited and fall behind the capacity of threats [25]. Attackers frequently target the path of minimum security with low resistance which leads to the unintended vulnerabilities caused by the human-aspect. Thus, cybersecurity threats that targets the vulnerability of human behaviour are at its consistent development and creatively advancing [22]. CSIS suggested basic cautionary that could enhance performance namely critically conformed cyber hygiene, effective planning, and “greater awareness among employees of the impact of the cyberattacks” [27].

2.2 Capacity Building in Cybersecurity

Capacity Building on its simplest form is a people-centred human development approach design to promote change and implies “a long-term investment to people and organization” [28]. It is also seen as a platform that can improve an organization's effectiveness and sustainability according to NGO Management and Policy Journal as cited in [29]. Zine Homburger defined capacity building on cybersecurity as “support and assistance” by strengthening and empowering individuals, communities, and governments to mitigate risks which a result of poor access and utilization of ICT” [30]. Efforts driven to cybersecurity capacity building are design to tackle broadening impact of threats and actual crimes in digital space [31].

Various initiatives to support cybersecurity capacity building were designed and shared among nations and organizations. Global Cyber Security Capacity Centre identified “building cybersecurity knowledge and capabilities” as one of the five (5) dimensions that form the methodical framework of cybersecurity capacity maturity (CMM) model for nations [32]. Dutton, et al, identified the “knowledge development” among the six (6) area focus of the cybersecurity capacity building [33]. This involves initiatives in education, training, and building and strengthening skills, and sharing of good practices. Identifying key actors furthering development of awareness campaigns and training should be done strategically to achieve desired results of the focus area. World Economic Forum (WEF) networked readiness pillars include a robust educational system building workers with the requires skills [34].

In one of the seminars on capacity building in cyberspace of European Union Institute for Security, they have generally agreed that “capacity building should allow recipient countries to harness the skill needed to be able to enjoy and reap the benefits of cyberspace with economic and social domains” [35]. It is a more encompassing term of building and strengthening the knowledge and awareness of the target recipients in the context of cybersecurity. EU commits itself to work on various initiatives to foster “cyber resilience, safeguarding the communication and information, ensuring the cyberspace community and economy protected” [15].

With the campaign banner “cybersecurity is a shared responsibility”, EU unites its citizens on its combat against cyber threats [36]. European Commission launched its recent Cybersecurity Strategy in 2020 which covers the building and strengthening “capabilities to respond to extreme cyberattacks” [15]. ENISA and CERT-EU forged a synergy to assist member states and EU institutions on operational cooperation, knowledge and information, and capacity building [37].

NATO CCDCOE promotes and provides lifelong learning in cybersecurity and courses based on the recent studies and cyber defence drill [38]. The training portfolio that they offer includes the strategic, operational, legal, and technical. These can be accessed in various platforms/ formats and settings. It might appear intimidating and only for the IT and cybersecurity experts and experience, CCDCOE also provides cyber defence awareness through an e-learning portal. This focuses general information on cybersecurity, specifically, attack methods, terminologies, and defensive mechanism [38]. The institution targets to reach the general public or the “average users”.

2.3 Learning to adopt Change

European Agenda put forth the adult learning and open education as key elements of campaigns and focus [39]. “Opening up Education” as perceived in the paper of Munoz-Castano et. al, can enhance the adult learning in Europe [40]. The same paper argues that “education and training systems” need to provide, if not fully resort, innovative recourse to aid various challenges Europe is facing.

Human capital theory presents consequence of competence through time- it expires and depreciates [41]. Adult learning covers the “formal and non-formal learning” after the initial education and competency training professionally or personal development [42]. Supporting the capacity building on the education, training, and awareness should always consider the profile of the audience or learners of the intervention. In this case, public sector employees/ staff who are on their adult years. Theoretical foundations are consulted as framework for various learning experience and platforms to ensure the effectiveness and efficiency.

Adults learn best in an “interactive setting with focus on the practical application of acquired knowledge” [43]. According to John Dewey, one of the foundations of experiential learning, “individuals have the ability to flourish throughout life” as cited in [43]. It is understood that life-long learning focuses on the knowledge acquired through experience. Malcolm Holmes sees human beings of having “innate tendencies of learning as people mature” cited in [44]. Accumulated “life experiences and knowledge” of adults are deemed to be connected with these stocks of knowledge and experiences [45].

Erik Erickson noted that adults seek meaning and purpose [43] [45]. According to Erik Erickson on his psychosocial moratorium, people are becoming creative when they feel there are no social drawbacks to making mistakes [46]. An environment of which mistakes are not a mistake but a try again encouragement to arrive in the desirable state, this is evident on what games could offer. Motivational theories are deemed as basis for a “life-span development” [47]. Cognitive scientists elaborated that the failure to conditionalize knowledge is the lack of ability to apply the acquired knowledge. The opportunity for transfer of knowledge becomes irrelevant in the perspective of the learner [48]. Janet Eyler stated on her featured article, The Power of Experiential Education, “deep understanding allows transfer of knowledge and for it to be useable it has to be learned in a situation” [49]. With the intervening responsibilities at work and with family or personal lives, adults are facing barriers in participating in learning. Thus, enhancing their reasons to start and sustain learning became the perpetual mission of organizations and academe.

Motivation plays a key role to enhance the learning experience of learners or user of a system/ webpage/ application. Stephen Lieb identified six (6) factors of sources of motivation, to wit, (1) social relationship (making new friends, networks), (2) external expectations (fulfilling expectation or recommendations from an authority), (3) social welfare (serving mankind/ community), (4) personal advancement (professional development, improving oneself to compete in a job), (5) escape/ simulation (break from routine of work and personal life), and (6) cognitive interest (seeking higher knowledge, satisfying an inquiry of mind). The self-determination theory elaborates the role of competence, relatedness, and autonomy as key elements that motivate a person to do a creative work [50]. This theory presents that individuals are not only motivated to do a certain task or a thing with rewards and punishment.

2.4 Cybersecurity Awareness Training

Chris Leach of CISCO viewed 2020 as a year that made the world realized the role of the resiliency amidst the pandemic. Leach suggested three (3) main areas organizations should focus on to mitigate the risks, "policy consideration, security awareness training, and risk evaluation". According to Peter Grabosky (2015), as cited in the study of Chang and Coppel, one of the most relevant strategies in the "prevention and mitigation of cybercrime" is the public awareness raising on the recurring risks for both individuals and organizations [16]. This is in support to various segments of strategies namely framework in place in the form of legislation to criminalise broader types of cybercrime, harmonization of international law as well as global cooperation in the development of capacity to deal with cybercrimes [51].

Changing landscape of cyberspace threats can be effectively solved and aided by the appropriate training [14]. This is deemed crucial particularly the disseminating of information among the members of the organization. This typically means the traditional and mainstreamed channels to "communicate security requirements and appropriate conduct" towards a cybersecurity threat [52]. Training may contribute to the immediate increase in knowledge on the subject matter, but long-term outlook of the recipient does not always follow [53].

In a special publication of NIST, it is explicitly highlighted that "awareness is not a training" [54]. The same report elaborates that an awareness presentation should allow the individuals to "recognize IT security matters and respond appropriately". Cyber risks are effectively aided with awareness and appropriate behaviour towards the threat. Cybersecurity awareness campaigns mainly aims to support and influence the assumption of "secure behaviour online" [52]. It is a learning process that provides learning environment "by shifting individual and organizational behaviour" towards learning the importance of cybersecurity and its impact [55].

According to Jagjhot Bharddwaj there are “significant number of the cyberattacks are due to lack of awareness and know-how”. Different techniques may have used by the attackers which cause harm to an organization in different ways [12]. Significant occurrences of cybersecurity attacks originate from inside the organization mostly due to the ignorance of users’ and careless practoces such as sharing passwords and opening unknown e-mails and attachments [22]. “Ensuring the appropriate coverage of security awareness topic” are deemed as an important task at hand, however, the key success factor for a security awareness initiative lies in the “delivery methods” [56]. Nevertheless, awareness and implementation of certain policies are known best solution to tackle cyberattacks [12].

These awareness campaigns usually involve “lectures or presentations” imparting the emerging and recurring issues to students and employees [57].But the design for this platform remains obscure depending on which perspective the learning method is based, “presenter and time- conscious oriented” or “effective transfer of information” from recipient’s point of view [14].

The existing strategies to disseminate the cybersecurity awareness highly depend on the cybersecurity message, and resources available to conduct the campaign namely “web-based session, computer-based session, teleconference, instructor-led, and cybersecurity days/ weeks. Months events, posters, and social media post on warning messages, newsletter, knowledge café, recognition or incentives program” [58]. Bada, et al, considered the form of the materials (interesting, current, and simple) used as key for an effective awareness and training program. Critical learning details in implementing the cybersecurity awareness are repeatedly missed out, to wit, [59] [60],

- Users’ absorption and retention capacity
- Stress levels of the individuals affect the decisions made in a cyber attack
- Highly technical nature of the topic tends to be boring
- Recognition and incentives for users who maintained an effective cyber hygiene. Most of the programs tend to focus to those who commit mistakes
- Increase of learning, a before and after measurement of learning outcome

Another type of educational technique became the go-to or viable option for some of the organizations, experiential learning. It is a technique which learner is directed towards the realities of the concepts [61]. These are being understood using real-life scenarios of which these concepts are being situated. One of the popular methodologies used in cybersecurity education is learning by doing approach [12]. A type of experiential learning found to be more effective and engaging than usual slide presentation and multimedia videos, serious games. In Jagjhot Bharddwaj study of "Designing a Game for Cybersecurity Awareness", serious games were used as it is deemed to be more effective and engaging [12].

2.5 Public Sector on Cybersecurity Awareness Training

Michael Barzelay emphasized on his book design-oriented professional discipline how does the professional competence coincides with the main purpose of public organization. Professional competence forms part of the bigger and complicated mechanism-intent chain to achieve public value while ensuring end users' benefits, satisfaction, and added value to their identified needs [62]. In the past decades, many of the eGovernance initiatives focused in "citizen-centric focus" or the government to clients, business, and government digital transformation [63] [64].

The government to employees (G2E) model describes the innovative solution to improve the communications and coordination among government units and employees, and access to information and learning opportunities. This model also explains the effective way to innovate learning opportunities and environments such as e-Learning, and knowledge sharing [65]. According to Golubeva and Merkuryeva, G2E seeks to improve its function by increasing the proficiency of the "public sector's internal work performance" [66]. Using a multistakeholder inquiry, the findings contributed to the creation of a single common platform for cybersecurity awareness programs in Malaysia [55].

Estonia actively promotes their cyber security hygiene. In 2017, the Information System Authority and CybExer Technologies (cybersecurity company) launched the DigiTest. It is a cyber hygiene training platform for the employees of the public sector [67]. The Cyber Security Report for 2021 indicated 15,000 users who have completed the test. The platform intends to increase awareness of the public sector to prevent small to larger cyber-attacks. The platform doesn't only cater for the employees of the public sector in improving their cybersecurity awareness, it also helps RIA to identify weak points based on the profile of learners in the platform.

The Cyber Security Agency of Singapore is at forefront in protecting Singapore's cyberspace. Its core mission is to keep the country's digital space "safe and secure" for a continuous delivery of vital public services [68]. The country released the Safer Cyberspace Masterplan for 2020 which highlights the primary thrust of the CSA which includes the empowerment of Singapore's "cyber-savvy citizens" by strengthening each cyber posture. Continuous campaigns with various platforms and formats were released for the public. CSA have compiled various platform to disseminate the awareness and ensure the agency will be reaching various types of profile.

2.6 Game-Based Learning

Game-based learning or GBL relates to the "process and practice of learning by using games" [69]. A known product of this learning method is called *serious games*. It is a type of experiential learning utilizing "entertainment and simulation" aspects as a process to present particular "learning objectives and incentivize the players in the journey of the game (from decision making to solving a mission) [70]. Its defined potential as a learning technique or pedagogical benefits has gained a lot of attention from academe and industry [71]. Yu-kai Chou mentioned on his book, Actionable Gamification, how games are the human-focused designs. Humans are building blocks of "emotions, ambitious, insecurities, and justifications to start/continue/ end doing things [72].

According to Mihaly Csíkszentmihályi, individuals are hooked in various activities because of the sense of enjoyment felt while doing a part on a preferred task or which is known as the flow theory [73]. This theory tackles the cognitive features of a certain experience focusing on the relationship of the player's skill level and the difficulty or level of challenge a task presents. The difficulty of the task highly contributed to the increase of the players' skills. But it also affects the anxiety level. Difficult challenges require higher skills level, otherwise, anxiety goes up which highly results to the early dropout in the task or activity. To sustain one's motive, elements such as focus, goal, control, feedback, transformation of time are considered. The flow theory explains the relationship of anxiety and skills to sustain one's motive. Elizabeth Boyle noted on her study that playing games causes the feeling of enjoyment [74].

Games According to Nicole Lazarro, brings fun and considers a key motivation to learn. Every component of enjoyment has four (4) types, "hard fun, easy fun, serious fun, and people fun" which allow the learners/ users to sustain the desire of continuing a task [75].

While Hook Model presents the users/ customers’ problems should be connected to company’s solution with enough frequency to create a habitual behaviour [76].

GBL is being sought as a workable option among available delivery methods in raising awareness [22]. “Games and simulations are attracting attention as having enormous potential as powerful teaching tools that may lead to an “instructional revolution” [59]. Catherine Becker created a “magic bullet model” or the four (4) categories of learning in games, (1) “things we can learn; (2) we must learn; (3) learning from a result of playing the game but are not intended in the game; (3) learning beyond the game which are helpful in the game itself” [77].

An effective game design concentrates on the player experience by creating a goal that “allows the player feel motivated” [58]. “There are eight game genres defined by Adams such as “action, exploration, role-playing games (RPG), sports, vehicle simulation, strategy, construction and management simulations, and artificial life and puzzle” [12].With growing acceptance as a viable option in learning, limited literature and documented experience found in the discussing the use of this learning technique in the public sector. Like any other organizations, public sector requires continuous learning and capacity building most importantly to those newly found fields or recently considered important spectrum in the digital transformation such as cybersecurity.

UNESCO recognizes how not only fun but highly educational video games can provide. The gaming initiatives of the institutions aims to utilize the “power of play to go beyond national boundaries, sharpen problem solving skills and foster the emotional space of empathy” [78]. UNESCO MGIEP supports the promising new-found pedagogy from GBL. They have developed two (2) games namely, World Rescue, and Cantor’s World. Eventually, the institution resorted to maximizing available online games by evaluating short-listed games based on the standards and targets they are aiming for. This strategy is the result of limited funds of the institution for this type of initiative.

2.7 Public Sector on Games

Public administration by nature is a risk-averse institution [79]. Decisions and strategies are made with utmost consideration or reference to the previous successes it brought for the public sector. Game-based learning for public sector may sound appealing but may also see as inappropriate style of learning for some because of what it is called. For one, serious game is named as ‘serious game’ as an “assurance against misguided minds from those who are new to it [70]. One study documented how serious games have gained support beyond gaming society. According to David Crookall, the French government, U.S.A Institutes for Health, and E.U. for the GaLA network are providing assistance for the advancement of serious games [70]. But still, documented practices of public sector on game-based learning are extremely limited to none. In Mateo Hernandez and Julian Moreno study, among 60 studies, only one (1) article discussed game-based learning being used in the government [80]

The elements discussed are important to analyse on its own to fully understand the very nature how these can complement each other or be workable as a capacity-building. And finally, these elements will be contextualized using the lens of public sector. Framework will be used to further understand and explain the context of certain element and possible implication to each other’s core.

2.8 Game-based-learning on Cybersecurity Awareness Training

Serious games as a platform for cybersecurity awareness/ training are relatively new which mostly cater to children, teenagers, and student [10] and others mainly focusing on the identified experts in the field. The same study of Hendrix et al, found these games free of charge and of short-term use which is contradicting to the end goal of long-term cybersecurity behaviour. Limited games found on the internet or studies that caters a game-based platform and with cybersecurity topic. It also ranges from various level of topic from experts, decision makers, and K-12.

Limited search was found for Adults as audience of the game. This is a critical found information as adults usually have the access to the important information and infrastructure that contribute to cyber risks. While both ends of the spectrum, top decision makers, experts, and children and young adults are the target of the available games online, a wider gap exists for mature adults. Games are still seen as play or something very specific use for specific profile of users.

3 Research Methodology

The present study seeks to understand the motivational drives behind human behaviour, desire, and needs [81] in the course of the cybersecurity awareness using game-based learning. It targets to capture a more meaningful and in- depth inquiry and analysis of the human tendencies towards learning cybersecurity. The primary investigator will answer the research questions using *inductive approach on the qualitative data collection and analysis*. "Inductive approach is a systematic approach for the evaluation of qualitative data" [82]. Responses or transcripts from the participants and available literature from vast databases and published peer-reviewed articles are analysed and transformed to themes then to contextualized findings [83].

The inductive approach allows the results to surface from substantial themes inherent from the raw data. This approach will enable the formulation of clear links and association between research questions/ objectives and the findings captured from the raw data [82]. Inductive approach also entails the formulation of theory(s) from captured data [84] [85]. It presents details which are not predetermined categories or focus, "sensitivity to the contexts", and interest to the impact of researchers and respondents' values [83]. Specifically, the chosen research methodology allows the researcher to analyse patterns, theory testing, exploration, comparison, or evaluation to understand a phenomenon [86].

Qualitative method intended to capture depth of understanding while ensuring the ability to "compare and contrast", likeness and peculiarities of an interest [87]. The thesis seeks to understand the experiences of the experts, implementers, and users/ learners on cybersecurity, cybersecurity awareness, serious games, and adult learning in the public sector. Primary data will be non-numeric mainly coming from cybersecurity games found online, interviews and focus group discussion extracting observations, and actual words of the identified participants [83]. Cybersecurity online games will be identified using the search/ word parameters which will be run in google search and documented in various studies. The empirical evidence from the purposively identified participants in the data gathering is highly considered in the thesis. Thus, it is systematic to utilize the inductive-qualitative approach as research methodology of the thesis.

3.1 Octalysis

Various frameworks are seen in the vast literature available online explaining the effectiveness and efficiency on the use of game-based learning approach. Most dwell on the behavioural theories/ frame; self-determination theory [50]; 4 Keys 2 Fun [75]; Player types [88]; the flow theory [73]; Hook Model [76]; etc. are being used to explain the human tendencies and motivational foundation on the learning experience.

Specifically, this study will utilize *Octalysis Framework* to fully understand the context and core drivers of the existing digital game-based available in online platforms. Octalysis came from two words of "octagon" shape and "analysis", thus Octalysis. Each side is representing human behaviour/ motivational foundation which is referred in the framework as core drive. The eight core drives are the overlapped behavioural frameworks of self-determination, 4 Keys 2 Fun, Bartle Player types, The Flow, and Hook Model. This framework has been used in various fields but limited in tackling cybersecurity awareness. It is formulated as framework in creating a gamified experience/ gamification for non-game fields. While game-based learning and gamification are two different system, both share the use of game elements to improve the experience.

This specifically explains the behavioural and motivational dependencies of individuals working for public sector towards learning approaches they go through. This framework is a product of continuous search to understand the drives within individuals to "motivate humans to pursue activities or endeavours" [89]. The framework suggests how online games became interesting and fun to engage with. It specifically implies certain core drivers within humans that stimulate individuals to pursue activities [90]. Diagram 1 further explains the process and frameworks that will be used in the study.

Chou refers Octalysis as a Human Focused Design. It is a "system to optimize the motivations and feelings of the human inside which particularly focuses on the understanding of the users/ learners' motivation to engage with a certain experience" [72]. Specifically, it seeks to recognize the "feelings, insecurities, and reasons behind the urge of doing things". These fuel up and sustain the motivation and engagement towards a certain thing. The framework has presented three (3) various levels of understanding optimization of motivation. For this thesis, the researcher will use the Level 1 and Level 2 frameworks.

In Chou's Octalysis Level 1 [72], there are eight (8) core drives that motivate a person to do certain things, to wit,

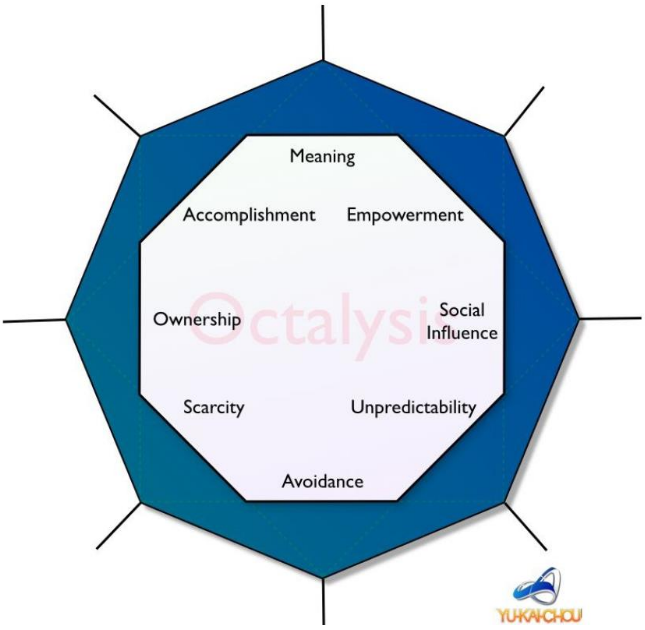

Figure 1. Yu-kai Chou' Octalysis Framework- Level 1

Epic Meaning and Calling

This core drive makes a person considers that playing the game is a contributing to greater calling or providing a meaningful share of actions towards an advocacy. It also describes how does a person believe on his/ her innate ability only he/ she has.

Development and Accomplishment

This explains the individuals' motivation for progress, skills development, attaining mastery, and overcoming a challenge. Person enjoys achievement and recognition of hard work or just even luck.

Empowerment of Creativity and Feedback

Individuals feel empowered whenever the circumstances allow them to be creative. This core drive describes the human motivation to be heard and allowed to decide on certain matters. As individuals are empowered to call the shots, it is equally important for them to receive feedback on how they have performed and adjust accordingly.

Ownership and Possession

It highly motivates people if an environment allows them to "own and control". This is highly evident when learners create their own avatar/ character in the game. It makes them feel that the character playing is more of themselves and not just a character made for them. As we progress in the track of the game, challenges or the journey allows you to accumulate virtual goods through hard work or by luck. It gives the learner the feeling of possession and desire accumulate more.

Social Influence and Relatedness

This entails all the social elements that drives individuals which includes "companionship, competition, and envy)". Humans are social animals. We seek that community or sense of belonginess (clubs, exclusive groups, membership, etc.). Some also thrive with competition which motivates the learners to be better than others.

Scarcity and Impatience

This core drive motivates persons to want and seek for more because of the (1) exclusivity of the item, and information; (2) rarity of chances to acquire certain things (time or certain points). Humans become eager to finish a task or impatient to take shortcuts (paying for the convenience).

Unpredictability and Curiosity

Individuals tend to try out a goods or services if it has that element of surprise or uncertainties. This core drive ignites our curiosity of what will happen next or what in the end of the line. It keeps us moving forward because surprises and uncertainties push us unravel what is next.

Loss and Avoidance

This motivation dwells to the individuals' fear of losing of anything. This can be time, resources, or possession acquired while playing the game. Individuals will try to avoid this loss even it means getting more from them.

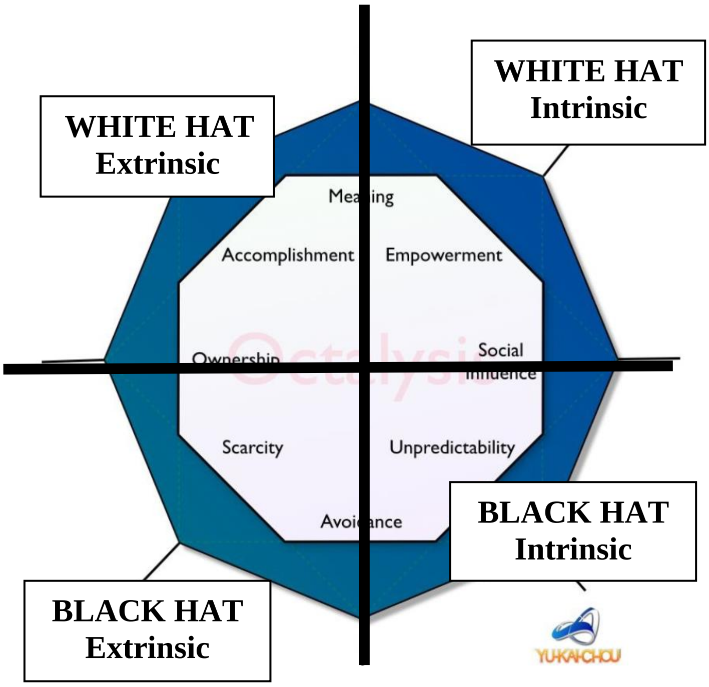

Figure 2. Yu-kai Chou's Octalysis Framework-White/Black Hat, Extrinsic/ Intrinsic Motivations

Among these core drives, Yu-kai Chou identified positive motivations and core drives leaning to harmful side, White Hat and Black Hat, respectively. White Hat motivations techniques leads to the development or shared contribution for the world, organization, chosen community, resources, or oneself. It entails to further an interest for the betterment but without the sense of urgency. These set motivations are the ideal state of a feel-good game. It allows learners to "express creativity" with the sensation of "unlocking or achieving certain level of mastery" while keeping the utmost "sense of meaning" which eventually lead you to "feeling better" and "in-control" mood. Topmost core drives in the framework, Meaning, Accomplishment, Empowerment, Ownership (part), and Social Influence (part) are described as White Hat.

Black Hat are motivations that drive individuals to do things that are seemingly urgent and feel lack of control of one's behaviour. The bottom of the framework, Scarcity, Avoidance, Unpredictability, Ownership(part), and Social Influence (part). This side of the Octalysis is not necessarily negative motivators [72]. It drives individuals to do more because of the "uncertainty hype" it brings in the situation, who does not want surprises if it is something that can bring joy eventually. Individuals always allow themselves to be subject in a competition to oneself but mostly trying to be better by proving something to another individual or situation. This also allows human instinct to get into the system of individuals. It gives the learner the sensation of pride when desired state is achieved.

This part of the Octalysis also involves the "constant fear of losing of something" that you might have acquired during the challenges or by luck. The learner might lose the grip of these things because of the exclusivity or the pressured environment or process before having or keeping that something. This game state describes the adrenaline-rush and all the hormones-rush as you try to succeed on the task. It might feel good at first but mostly if done every time, according to Yu-kai, might leave a "bad taste in your mouth".

These core drives are also classified to Extrinsic and Intrinsic motivations. According to Chou, extrinsic motivations or the left side of the framework have originated from "goal, purpose, and reward" while intrinsic motivations or the right side of the Octalysis are simply motivations to enjoy doing a task [89]. He also added that core drives found in the left side of the framework are goal- oriented while the right-side leans to an experience-oriented nature, hence extrinsic and intrinsic, respectively. Hennessey et. al., defined intrinsic as "the motivation to do a thing for the sake of enjoying the task" and extrinsic as drive "to attain external objective or target" [91].

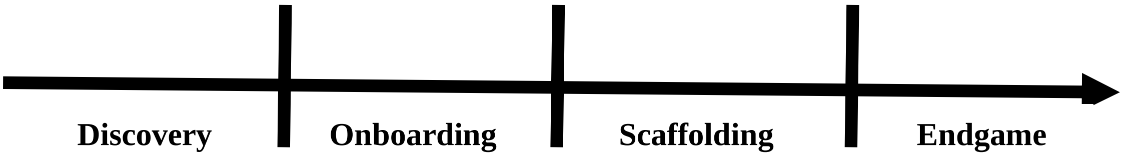

Figure 3. Yu-kai Chou's Octalysis Level 2

Octalysis describes the learner’s or user’s journey.

[72]:

> **Discovery** pertains to the methods how did the user came to know about the experience. In most of the training in public sector, discovery of the experience is happening because of the compliance or mandatory cascade of the experience. After which, **Onboarding** starts to present itself. This involves learning the rules and ways to succeed in the goal of the game. This part more likely starts in the creation of account or registration, test space, a quick briefer (in text or video), etc. The actual start of the journey is the **Scaffolding**. This may be repetitive tasks in different places in the journey to achieve a certain goal. Then, the journey reaches the **Endgame**. This is keeping the individuals/ users in the experience of a system, applications, platforms.

Among the searched peer reviewed studies in google scholar, scopus, IEEE Xplore, and ScienceDirect, Octalysis is mainly used to innovate and sustain the experience of a user/ learner using game elements. A dynamic game was developed to improve teaching methodologies using the accomplishment core drive in the Octalysis Framework [92]. Known online selling sites were assessed having core drives based on the Octalysis, game elements have embedded in the sites’ processes with above 50% presence [93]. Games found in Google Play Store were evaluated what are the dominant game elements and match this with the found motivational core drives [94]. Among these games, 7/8 core drivers are found to be present. It also formulated a matrix of game elements vis-a-vis core drives usually present into it.

3.2 Data Collection/ Sampling technique

Sampling technique for the present study utilizes procedures commonly used and systematically proven for social and behavioural sciences. Purposive sampling techniques or qualitative sampling involve the selection of “certain units or cases” [95] and highly founded on the “specific purpose rather than a random procedure” [96]. Samples are targeted from which the researcher will learn the most based on the experience and expertise established by the key informant. This targeting mainly describes the reputational sampling under the purposive category.

To gain understanding on the core drivers of the existing digital serious games on cybersecurity (RQ1), a desk review will be conducted. Games on cybersecurity awareness will be identified through an online search. The terms searched will be "cybersecurity awareness games", "cybersecurity games for adult", "cyber awareness games", "cybersecurity games for public sector". The search will focus mainly on the games implemented in EU, public sector, free web-based, and popular downloads (by ranking or popularity) and as captured in various studies.

Some of the sites where the searched will be run:

- Google search
- Google Play store,
- Gaming sites (Gamesspot.com/ Steam) and
- As documented in various studies

The inventory of games will be listed in a table with its basic profile (game genre, objectives, etc.) and aligned with the core drives and to which game elements it was found. The Octalysis and Sillaots Mapping matrix from the study of [94]. Octalysis Framework (Level 1) will be used in the inventory of games.

Online games dealing with cybersecurity awareness are available in various sites. These games may be free all throughout the game, free to a certain extent, exclusive use per request for a limited access, or paid version of a game all throughout. Games for cybersecurity awareness specifically for adults are systematically searched and assessed. The results of the assessment will present an overview on the game design used and prioritized in the entire journey by identifying the core motivational drivers in place vis-à-vis user/ gamer journey phase. It will be an inventory of cybersecurity awareness games and profile of each game when it comes to motivational drivers.

For RQ2 and 3, purposeful/ purposive sampling strategy will be utilized as the data collection technique known and proven procedure utilized in a qualitative research methodology [97]. It identifies individuals or groups that are known experts or "especially knowledgeable and experienced" with the chosen field [87]. Snowball purposeful sampling will be employed for the key informant interview and focus group discussion [98] [87] to obtain leads of experts and experienced individuals on the identified fields and eventually expand the initial list of key informants. The researcher started with the experts/ implementers from Estonia, EU, and e-Governance Academy dealing with National Cybersecurity Security Index ranking (e.g., NCSI).

Shifting the learning environment to another platform will always carry various key considerations for a seamless integration of the proposed platform and the topic it will be carrying. To assess the applicability and integration know-how of game-based learning to cybersecurity awareness to ensure and improve learning and learning experience experts and implementers knowledge and experiences will be collated. The interview will use a semi-structure approach in the interview. This will allow the process to be more free-flowing and less restricted for possible knowledge sharing.

Key informant interviews with the various experts and implementers in the fields of cybersecurity, cybersecurity awareness campaigns, and learning experience, game-based learning are specifically targeted to shed light on the harmonious collaboration and anticipated challenges in the merge. Specifically, experts on the implementation of capacity building on cybersecurity awareness in Estonia, European Union, and globally are targeted to participate in the Key Informant Interview (KII). Their expertise and experience will be woven to design a Users' Learning Experience using game-based method in cybersecurity awareness. The objectives of the KII, to wit,

- To understand the current landscape of cybersecurity awareness initiatives implemented (level of preparedness, awareness)

- To recognize the effective and efficient strategies among those initiatives (wins and challenges)

- To analyze the game-based learning and its environment for adult-learning experience (game mechanics/ design, wins and challenges)

- To assess the applicability of the game-based learning to cybersecurity awareness (risks, impediments, help/ support needed for the integration)

Questions were based on the expertise/ experience (cybersecurity, game-based design, capacity building, etc.) of the key informant. These questions were also pre-tested to verify the purpose, and clarity. Table 1 summarizes the profile of the KII.

Table 1. List of Key Informant Interview

Respondent	Scope	Interview Length
1. Cybersecurity Security Expert and lead implementer of cybersecurity awareness in the Public Sector (country level)	Estonia	56:31
2. Cybersecurity Expert and awareness raising and Education Team Leader (regional level)	European Union	34:53
3. Learning Experience Designer (global level)	UNESCO	51:52
4. Cybersecurity Expert (global level)	Estonia and Globally	32:05
5. Games for Learning Officer (regional level)	UNESCO	56:42
6. Cybersecurity Security Expert and lead implementer in the Public Sector (country level)	Singapore	1:07:39
7. Digital Technologies (Serious Games) Lecturer	Academe, Estonia	57:59
8. Cybersecurity Expert and Implementer (regional level)	European Commission	51:32
9. Cybersecurity awareness enforcer and learner (agency level)	Estonia	42:59
10. Digital Technologies (Serious Games) Lecturer and Experienced on the use of Serious games outside Academic curriculum	Academe, Estonia	1:15:21
11. Scientific Officer, Cyber and Digital Citizen's Unit and Game-based Implementer	Joint Research Center for European Commission	49:04

To directly influence the design of the learning experience, the study seeks the users'/ learners preferred experience that could optimize learning and sustain the learning experience (RQ 3). Users/ learners of the cybersecurity awareness training in the public sector of Estonia are targeted to participate in a focus group discussion. The result of the methodology will present preferred game design elements and motivational traits in place to reinforce learning and support learning process.

Clear understanding of the profile of the learners/ users while being certain on the topics that would be included cybersecurity awareness will help the thesis to come up with a user experience design [58]. Focus Group Discussion (FGD) is an exploratory technique which can help to inquire focused insights from target users on "what is already known and information on experiences that can be added to the already gathered or previously documented discussions/ findings on cybersecurity awareness" [55].

The objectives of the FGD, to wit,

- To understand the perception of the users on cybersecurity (organizational and personal)
- To analyse experiences on cybersecurity awareness and its direct contribution to their work and personal cyber hygiene
- To evaluate the users' game experience and perception (advantages and challenges)
- To assess the applicability of the game-based learning to cybersecurity awareness (goals, risk, impediments, and help/ support needed)
- To understand the motivational drives for them to sustain the use of a game-based learning platform for cybersecurity awareness

Target users are invited for a focus group discussion on cybersecurity awareness using game-based learning. They would be from a government agency in Estonia. The government office is purposefully identified based on the posed cyber risk to the functions of the organization. Employees of Social Insurance Board were invited and identified strategically by the middle-management KII participant.

Table 2. List of FGD Participants

Participant	Interview Length
12. Managerial-level, Accessibility	1.27.00
13. Managerial-level, Digital/ Innovative Solutions	
14. Archivist/Coordinator, Preservation	
15. Analyst, Business Requirement	

The interviews will be conducted via online platform (MS TEAMS) provided by the Taltech University. A collaboration board (jamboard) will be used to facilitate a seamless discussion and shift of topics on FGD. Trial board will be sent out to allow the participants to familiarize with the features of the collaboration board.

For KII and FGD, an initial communication will be sent out explaining the subject of the request, research goal, scope, discussion main themes, including the privacy and anonymity. Permission to record the session and the access to the file was explicitly discussed and requested before the start of the video recording. The video recording will only be accessible to the author of the study and the direct supervisor from TalTech. Gathered information and specific data leading to an identity are in no way be employed other than for the analysis of the findings of the study. The participation will be treated with utmost anonymity by default, unless participant(s) explicitly allowed and mentioned the permission.

Transcription from the Microsoft Streams will be downloaded. It is one of the Microsoft 365 products mainly on video service. This platform captures recording made from Microsoft Teams. Organizational accounts (e.g., Taltech) can upload, view, and share videos securely [99]. A transcription/ caption can be enabled with a choice of language to capture the interview in written form. VTT file cleaner [100] will also be used to increase accuracy of the captured transcription- more verbatim and actual words.

3.3 Data Analysis Method

Qualitative Data Analysis involves the “classification and interpretation of linguistic constructs, and statements to formulate meaning based in the contexts and what is represented/ evident in it” [101]. Through the texts researcher would be able to understand the participants’ thinking trajectory, feelings, and actions taken towards situations [83]. Russell Schutt reiterated that the meaning can only be subjected to the “consensual community validation”.

In the study of [94], a framework of Octalysis Core Drivers is coincided with Sillaots Game elements. The research analysed the present core drives in various game elements in several game genre including educational, simulation, and strategy. The Sillaots game elements are more elaborated on the original paper of Martin Sillaots et al [102]. The Octalysis and Sillaots mapping will guide the researcher on which part of the cybersecurity game to focus/ prioritize in validating the presence or absence of core drives. This will be used vis-à-vis the games searched from various sites to answer the RQ 1.

Table 3. Octalysis Core Drives and Sillaots Games Elements

Octalysis Core Drives	**Details**	**Sillaots Game Elements**
Epic Meaning and Calling	A quick briefer on what, who, where, when, how, and why of the game	Objectives Story Challenges

Development and Accomplishment	For every achievement, certain reward is activated	Outcome
Empowerment of Creativity and Feedback	The game allows certain capacity of the learner to choose its path and decide creatively. It entails feedback from the game.	Play World Build Boundaries
Ownership and Possession	The sense of belonging of various things/ items and ability to create an avatar or character based on the learners’ preference.	Resource Character
Social Influence and Relatedness	A built-in feature to be able to talk/ discuss with other players. This core drive also creates a sense of community towards the journey of the game.	Player
Scarcity and Impatience	Limitations set by the game builds the hunger and impatience of the learners.	Rules
Unpredictability and Curiosity	As game leads you to uncertain path, it allows the player to develop curiosity.	Random
Loss and Avoidance	Learners are driven to continue the game because of fear of losing (time, possession, or resources acquired devoted through the game)	Conflict Performance

For RQ 2 and 3, Thematic Analysis will be employed to better understand the transcription of the KII and FGD. Variety of software are available to support the analysis of qualitative data. Using these analytical tools increase effectiveness, efficiency, and accuracy of the data evaluation. For this thesis, NVivo version 12 will be utilized. NVivo, is continually developed and improved to support extensively the researchers. This software automates the sorting, matching, and linking of the themes [103]. It simplified the complex procedures to managing data/ ideas, query data, visualize data, and generate report from the data from manual method of highlighting and consolidating.

According to Braun and Clarke, there is a systematic process or phase of data analysis of which NVivo followed:

[104]

Engaging yourself with the data collected, transcription approaches and platforms

The researcher should run again the video recording to verify the veracity of the transcription from Microsoft Streams and VTT cleaner. This will allow the researcher to be acquainted to the interview done and important knowledge captured during the session.

Code your data

From the transcription, codes will be created based on the evident themes from the transcription while these coincide to the question asked during interview and relevance to the study. These will be the initial or general themes from the interviews.

Creating nodes (themes)

As the process gets into its depth, more specific themes will be identified as it embodies the thought of the data collated in that theme.

Reviewing your nodes

Themes will be reviewed to ensure cohesiveness and relevance to the present paper.

Naming your nodes

After reviewing your themes, themes might be merged final name of the theme would be identified. Merging and re-grouping of themes will be done to achieve a more cohesive line of thoughts and connections (similarities, differences, confirmation, and contradictions).

Making sense of the key concepts

These themes will be interwoven to other data gathered and formed a cohesive understanding of the data derived from interviews.

4 Results and Discussion

The search employed specific search parameters, “cybersecurity awareness games”, “cybersecurity games for adult”, “cyber awareness games”, “cybersecurity games for public sector”, and “employees”. These parameters were run in the various sites, Google search engine; Google Play Store; Gaming sites (gamespot.com, and Steam); Google Scholar; and Scopus. Within the set parameters, the search has collated limited variation of games, table 4 describe the profile of the game evaluated.

Table 4. Game Profile

Game	**Brief**
Targeted Attack [105]	- Trend Micro created a free online game where learners try to act as decision-maker in the Fugle company. It calls for immediate actions on the critical situations that lead to a successful or failed product launch. It follows a “choose your own adventure” of which every decision made will lead you in different path or worse compromised security systems if not corrected (multiple branches with various ending; replay-ability). - 5-10 minutes playing time - It provides a debriefing after the game from Trend Micro explaining what went wrong or how did every decision affect the end of the game
Keep the Tradition Texas A&M University [106]	- Division of Information Technology of Texas A&M University creates cybersecurity games every year as part of the National Cybersecurity Awareness Month. “Keep the Tradition was launched in 2017 to test learners’ knowledge on cybersecurity and Texas A&M traditions - It can be played interactively (location-based) or the online version

	- 10-20 mins (could have been shorter but loading of the game is slower) - On its launch in 2017, students and faculty from Texas A&M who would be able to finish the game were also part of a grand prize draw (apple watch) and gifts/ coupons (discount for apparels and meals).
Cybersecurity Games-CDSE [107]	- Center for Development of Security Excellence provided various delivery methods for security training. For cybersecurity awareness, they created several games which the organization actively promote to be utilized by other organizations. - The games are usually board/ tabletop games turned to digital game such as word search, crossword, spin the wheel, etc. - each game, 5-10 mins
Black Belt IT Security Training Game [108]	- Created by the company Centrigade. They have created the game as an alternative to the cybersecurity training. The game has strategically placed "intrinsic motivation" gaming elements. - 10-15 mins - It discusses spam/ phishing email identification (spam defense), identification of hacking possibility based on the information posted online (hack the planet), and handling and classification of paper-based and online documents (documents, please).
Cyber Siege (Can you keep your network alive) [109]	- This is a video game and tool product created by Naval Postgraduate School. It teaches computer and network security concepts and defense mechanism. - Learners are task to manage budget, productivity, and security. - Evaluation version of the game was used in this study. - 15-30 mins

Cyber land [110]	- This game is a product of the Cyber Security Challenge UK and National Crime Agency. They are making interactive online games available (free of charge) which are suitable for all ages and various levels of technical ability. - Cyber land puts you in to set of activities to test our (various places that are facing cybersecurity risks) the knowledge and skills of the learners on cybersecurity. - 20-30mins

4.1 RQ 1: Online cybersecurity games and its motivational core drives

Presence of motivational core drives and its strategic position were identified with the help of the Sillaots game-elements, and Octalysis core drives mapping from the study of Tobing et al. [94]. Table 5 summarizes the presence and absence of core drives on the evaluated cybersecurity games with specific game element.

Table 5. Game Assessment on Octalysis Core Drives and Sillaots Games Elements

Games	**Targeted Attack**	**Keep Tradition Secure**	**Cybersecurity Games- CDSE**	**Black Belt IT Security Training Game**	**CyberCiege**	**Cyber land**
Core Drives						
Epic Meaning and Calling	Objectives Story Challenges	-	-	-	-	Challenge
Development and Accomplishment	Outcome	Progress	Badges Sound	Badges/ Points	Progress	Badges/ Points
Empowerment of Creativity and Feedback	Play (gameplay) Support (Debriefing/ mentorship at the end of the game)	-	-	Support (Debriefing/ mentorship at the end of every task)	Play (gameplay)	-
Ownership and Possession	-	-		Character	Resource accumulation	-
Social Influences and Relatedness	-	Challenges	-	-	-	-
Scarcity and Impatience	-	Rules	-	Challenge	Rules	-
Unpredictability and Curiosity	Challenges Outcome	Challenge Outcome	Challenge	Challenge	Challenge	Challenge
Loss and Avoidance	-	-	-	Time	-	-

Online Games and Octalysis core drives

Targeted attack, CyberCIEGE, and Cyber Land provide simulation and decision-making exercise on resource management and critical organizational functions. Black Belt, CDSE, and Keep Tradition Secure focus on the conceptual knowledge through practical exercises such as quizzes, identification or spotting the mistakes. The motivational core drives found in the game were position strategically to trigger and arrive to a win-state of learning cybersecurity. Development and accomplishment and Unpredictability and Curiosity core drives are the common core drives among the six games evaluated. The least utilized are the Loss and Avoidance and, Social Influence and Relatedness though these were used by Black Belt IT Training and Keep Tradition Secure, respectively.

Targeted Attack

The brief about the game calls for a reality check in securing the cyber world. While organizations/ individuals are waiting it to happen, the (when), the game provides possible real-scenario (if) and its implications. It challenges learners to make right choices under various circumstances which might lead to success or a game over. Epic meaning and calling core driver are given with outmost importance. Its heavily distributed in the objective, narrative of the story, and challenges. It provides game-spiel which call to save the organization, thus, every decision made will have its implications. Development and accomplishment core drive can only be felt at the outcome of the decision made in the game, either you succeeded or have caused minimal to massive security implications.

Feedback core drive is not evident in the game itself. It is only provided at the end of the game through a debriefing. It provides comprehensive processing/ mentorship in every decision made and what could have made better. It also further explains the motives of every character, and cost implication in every decision made. And more importantly, it provides touch-based of reality while including efficient means or best practices to ensure the cybersecurity and minimize the impact considering all the circumstances at hand. The "choose your own adventure format or multiple branches with various ending creates the challenges and outcome with unpredictability and curiosity drive of what happens next or what would be the implication of the decision.

Keep Tradition Secure

It is originally meant for the students and faculty of Texas A&M University. 50% of the questions are related to the University's famous places. If you are part of the community of the University, it would be fun to answer the questions because of the social influence and relatedness motivation, basically questions that relate to the University. It would also be easier to move from one University related riddle to a cybersecurity awareness question if you are part of the University community. It seems like a walk to a memory lane, best for alumni of the and retired faculty of the University. Many of the questions provide immediate feedback or processing of the answers made.

The progress bar as monitoring of the development and accomplishment makes the slow loading of pages tolerable. The game leads you to various places to catch a character mentioned at the beginning. It creates a gradual excitement where will you be at every time you answer a question. This eventually leads to the core drive of scarcity and impatience as you are tasked to catch a specific character while answering cybersecurity questions while being led to various places in the University. Finishing the game for students and faculty of the University would mean a chance of winning gifts in real world. The unpredictability and built-up curiosity to where the journey leads you strengthen the core drive towards the challenges and outcome of the game.

Cybersecurity games (CDSE)

These games are created by CDSE created various games to choose from. Most of the choices tackle conceptual knowledge on cybersecurity. Three (3) among the available games are quiz type which have badges and sound add on to create a development and accomplishment environment for the learner. One game has the unpredictability and curiosity core drive using a spin-a-wheel to define which topic to proceed on the quiz.

Black Belt IT Security Training Game

This game enables you to create your own avatar (limited choices) to have a specific identity in the game. This activates the ownership and possession core drive as you create your character in the game. Each task provides processing or explains what the learner should be reminded of when it comes to the specific topic of the game. It is feedback core drive but not comprehensively presented. Every task puts you on a time pressure environment while making the greatest number of correct answers. The loss and avoidance core drive works evidently in this game element, losing the time while eager to accomplish more results. One task asks you to try analysing what would be the possible sources of password based on the social media post. This elevated your curiosity core drive if you have included all the elements that are possible answer to the task. The answer to each task is revealed towards the end of the game, it ignites your curiosity of what might be the outcome of the task.

CyberCIEGE

With given resource, learners are task to purchase and configure various IT devices and systems to protect the organization from cyber risks and possible breaches. Accomplishment is reflected through a status board which encourages the learner to prioritize available resource accordingly. The game allows you to be creative on your purchases while ensuring the security of the organization. Resource management builds the learners' ownership and possession core drive. Though there is no time limit, the entire game is being monitored to calculate how long does the learner solve the challenges. Allotment of resources to various purchases builds the unpredictability core drive as you try to save or minimize the risk of the organization.

Cyber Land

This game has presented various levels of challenges (beginner to advance level) which also from various set-up (school, café, work, industrial locations, and courthouse). In every task, the learner will take specific role (judge, investigator, IT administrator, etc.) to help each establishment get through the cybersecurity breach/ risk. This activates the epic calling and meaning core drive as you help each location and save or minimize their risks. Development and accomplishment are posted while you progress in the game through badges/ points. One of the challenges posed curiosity core drive while you choose one establishment to where you are task to help. Each establishment present difference challenges with different roles.

Figure 4 presents the mapping of the cybersecurity games to the Octalysis framework to visualize how does each game utilize the core drives; white/ black hat, and intrinsic/ extrinsic.

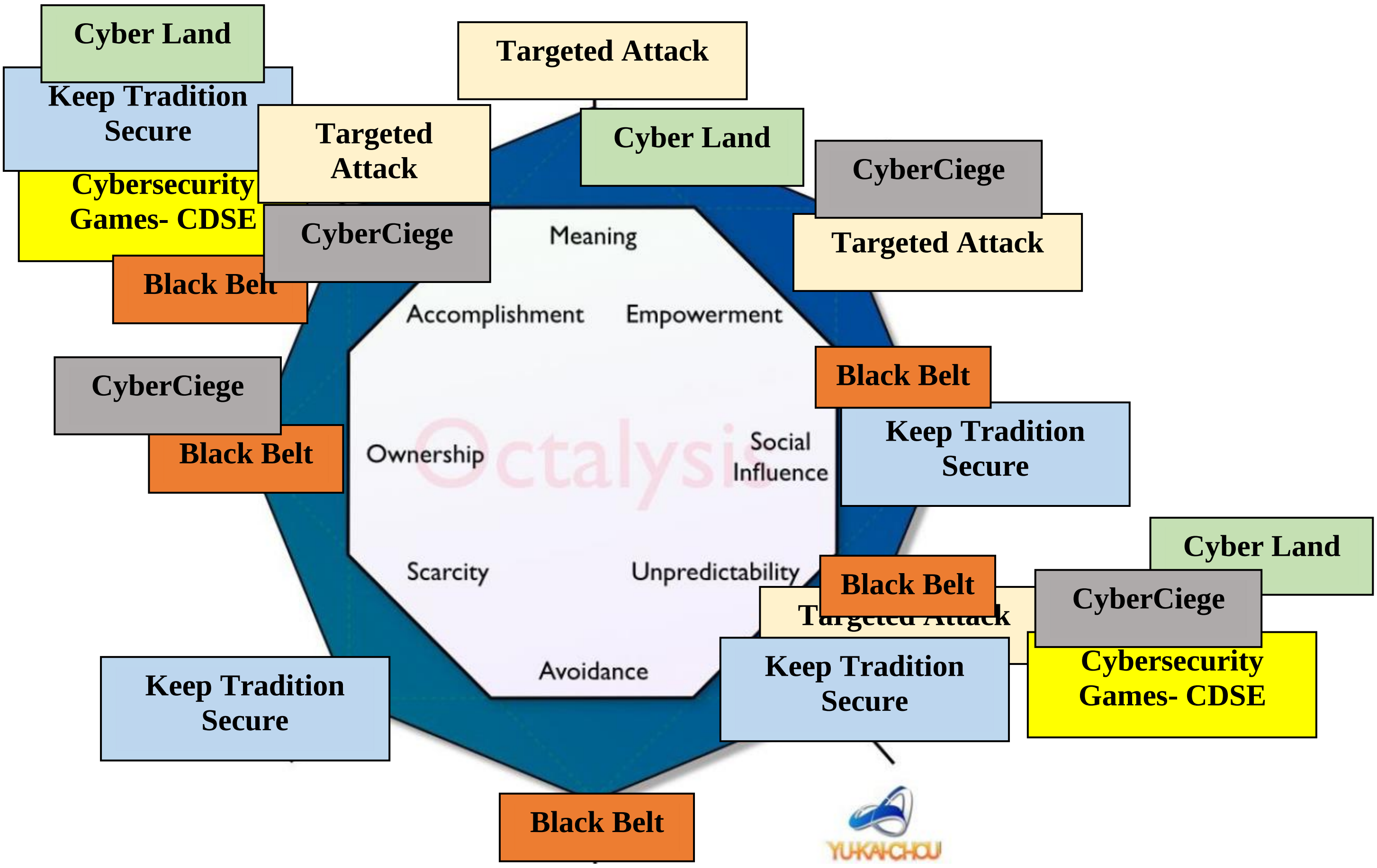

Figure 4. Mapping of Games to Yu-kai Chous's Octalysis Framework- Level 1

All the games have utilized white hat and black hat motivational core drives and intrinsic and extrinsic techniques. Targetter Attack utilizes the most the white hat core motivations. While letting the learner feel good about the game, the unpredictability of the path ahead and outcome makes the individual determined to finish the task. The surprise at the end will be reinforced with comprehensive feedback which allows the learner feels learned and informed. Keep Tradition Secure utilizes the four (4) quadrants of the framework by adding motivational elements from each side. This is seemingly a balance strategy but the positioning

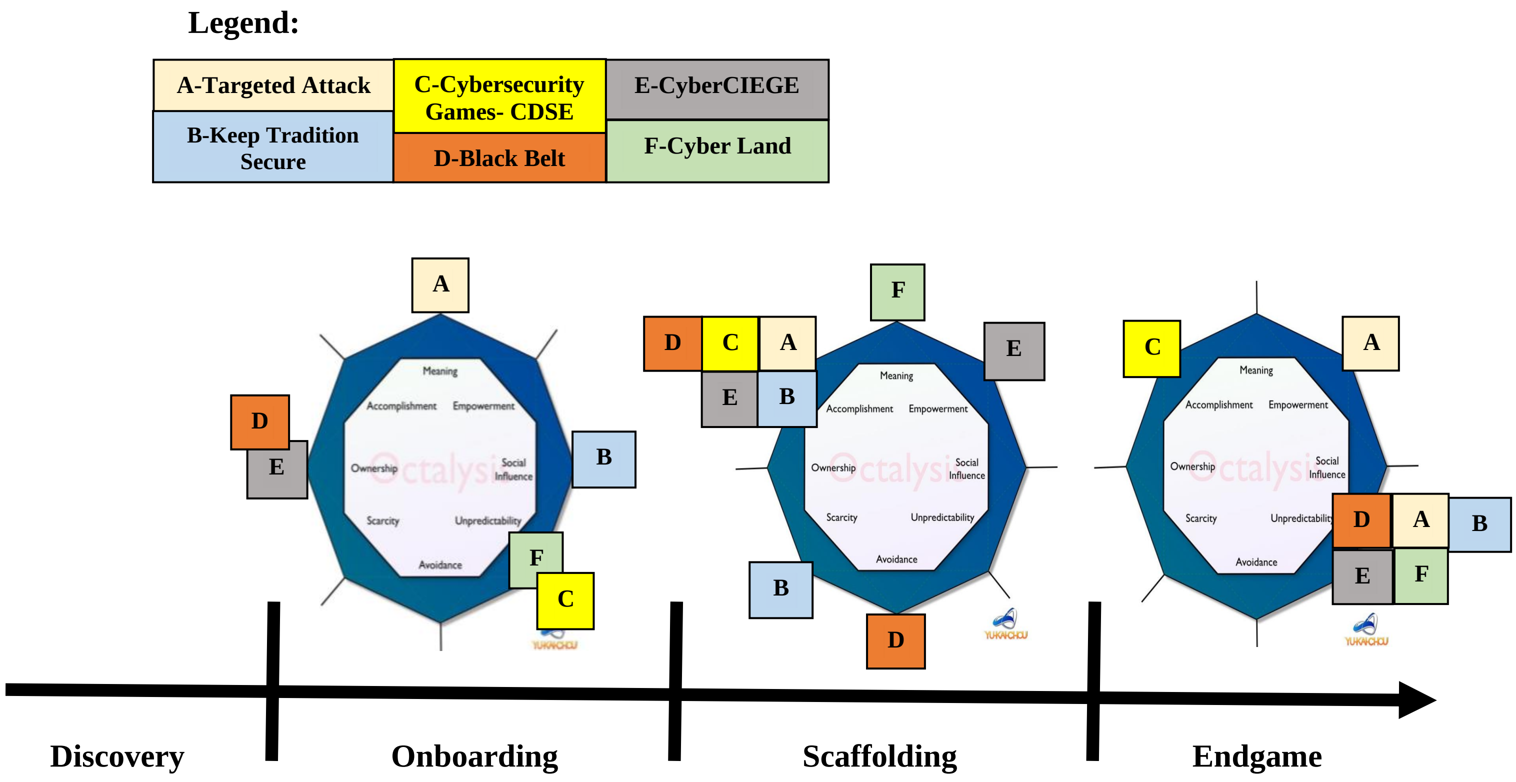

Figure 5. Aligning of Games on Yu-kai Chou's Octalysis Framework- Level 2

Discovery phase in the present study will not be applicable as every game is purposively searched for based on the parameters set. This phase is an important initial touch point to the learner as it sets the tone of the over-all journey or experience. It can be something you deliberately look for, fed to you by the artificial intelligence based on your history of searches on the internet, suggested by a friend or colleague or relative, seen in various sites (e.g. social media), or it can just be any other for compliance or mandatory tasks asked by your organization to complete. This phase builds the initial motivation to discover and get engage with an experience. Most training or organizational development in the public sector, if not all, are driven by the organizational initiative to improve its performance, thus, a compliance. This has strong hold towards of the journey of the learner. It creates a by-hook or by crook accomplishment of such because of the otherwise clause if the training is not accomplished. If this is the motivation for this phase, it can be classified in the "loss and avoidance" core motivation.

The present paper started the analysis of the cybersecurity games on its Onboarding phase. As learner already got the initial touchpoint to the experience or task, it is important to reinforce it with elements that will drive the learner to excitement and curiosity. The evaluated cybergames present an onboarding phase which leans towards intrinsic motivations. The specific explanation, to wit,

With epic meaning and calling in place, a call for action is presented to save or mitigate the risk an organization will be going through. It gives the learner a heightened feeling of importance and urgency. It creates a bubble of which the learner is the only person that can save the given situation. There is also a nudge to the learner for a great challenge ahead (are ready for it? Are you capable to do the task?). This adds another layer of challenge which fuel your eagerness. The game does not only call for you to save or help the functions of organization, but it also deliberately challenges your capacity if you can do any better.

Banking-on the social influence and relatedness gives you that nostalgic feeling or exclusivity while trying to figure out a case. This ignites the sense of relatedness as the game created a memory-lane journey. Provoking the sense of curiosity builds “what-if” and “so-what” inquiry to one’s head. It only drives the learner to move more in the journey of the experience. Management of resources or creation of preferred personal identity in the game allows learner to experience an immediate sense of control.

After the learner got onboard, the challenges begin or what the Octalysis called the Scaffolding. The transition from setting the tone and learner engagement to the challenges is critical aspect of the game. This is where the game begins its creativity by introducing the task or trying out repetitive actions that can be used in the challenges. 5 out 6 games are leaning towards extrinsic motivation and heavily used the accomplishment and development core drive. Boosting the experience by showing your progress or accomplishment creates a sense of fulfilment as learner sees the fruits of hard work. Preventing the learner to reach on the desired state creates impatience and might not be seen as an advantage through the journey. The use of rewards or accomplishment gauge could ease the feeling of impatience. Limitation of time to hurdle the challenges of the journey brings learner to a pressured environment which can ignite adrenaline rush and higher sense of competition. It would be a real rush after and sense of achievement if learner hurdles the task. The feeling of being informed or learned through feedback and empowerment puts the challenge into context and which brings back the learner to the main goal of the game, to learn.

After the repetitive actions or heart-pounding turn out of the game, the learner reaches the endgame. This phase determines if learners will stay, or it is the endgame. 5 out of 6 games utilized black hat intrinsic motivation. Allowing the learner to re-do or repeat the game now with other path or choices builds a sense of curiosity. This is an important element to present with the learners, the chance to improve the outcome of the process. An environment which radiates as a safe place for learners gives a sense of assurance of the real essence of learning, through the lessons learned. The way forward is to repeat the game towards the desired outcome after processing the lessons acquired. The learner does not only arrive in the win-state of the game, but also optimize the learning experience.

There is balance on how each game can design and position each motivational drive. Yu-kai Chou suggests on his book Actionable Gamification dominant strategies in utilizing white and black hat core drives in a workplace. According to Yu-kai, white hat core drives should be highly considered to allow employees to have a feel-good sensation while growing with the organization. This entails the establishment of meaning on the work that they do while mastering their chosen career with profound autonomy. Using the black hat is always an option with critical cautiousness. The compliance or mandatory model of cascading personal development for the employees of an organization can be seen as short-term and has superficial outcome. But instead of punishing the delinquents, organization should reward the employees for learning or using the platform for learning.

On the same book, Yu-kai quoted Micheal Wu of Lithuim on his recommendation to better entice and motivate people stay and enjoy the experience [72], to wit,

- Extrinsic rewards or motivation can attract and catch learners' attention
- While on the play/ learning, Intrinsic motivation such as "recognition, exclusivity, and status" can be adopted
- Long-term engagement can be ensured using an Intrinsic motivation

This recommends the importance of motivational elements and its position throughout the game. It cannot be effective and efficient if not strategically positioned in the entire journey of the game. One element or two will be short-lived if not reinforced with motivational elements that can complement and create a long-term engagement of learners.

4.2 RQ 2: Integration of GBL and Cybersecurity Awareness

The transcriptions for the Key Informant Interviews were downloaded as captions in the Microsoft Streams. Interviews are conducted in English. Transcriptions were also run on VTT cleaner to capture accurate audio recording of the interviews. After which, NVivo version 12 was used to systematically code and identify themes among the data gathered qualitatively.

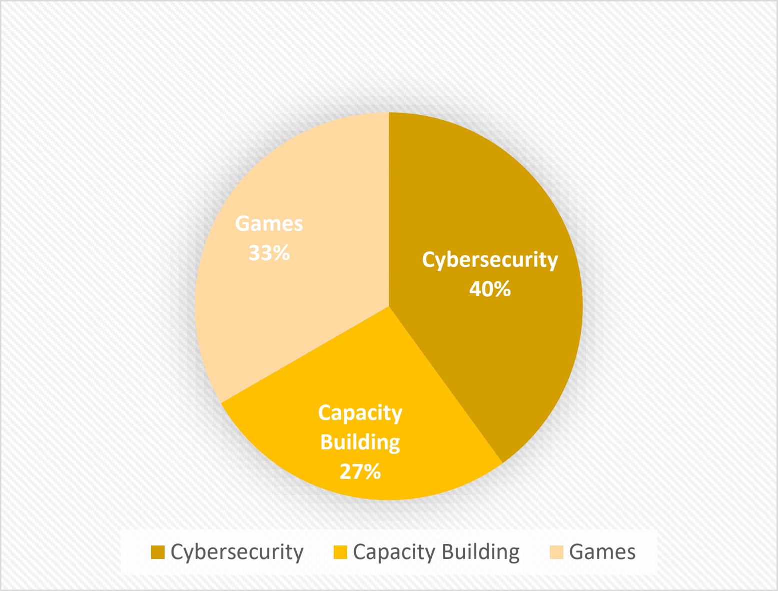

Figure 6. Distribution of KII participants based on expertise

The participants of the key informant interviews are mainly from the fields of Cybersecurity, Games, and Capacity Building and some overlapping experiences on Games and Capacity Building, and Cybersecurity and Capacity Building. The diverse and related experiences and expertise have helped in shaping the important points in the present study.

Cybersecurity amidst the Pandemic

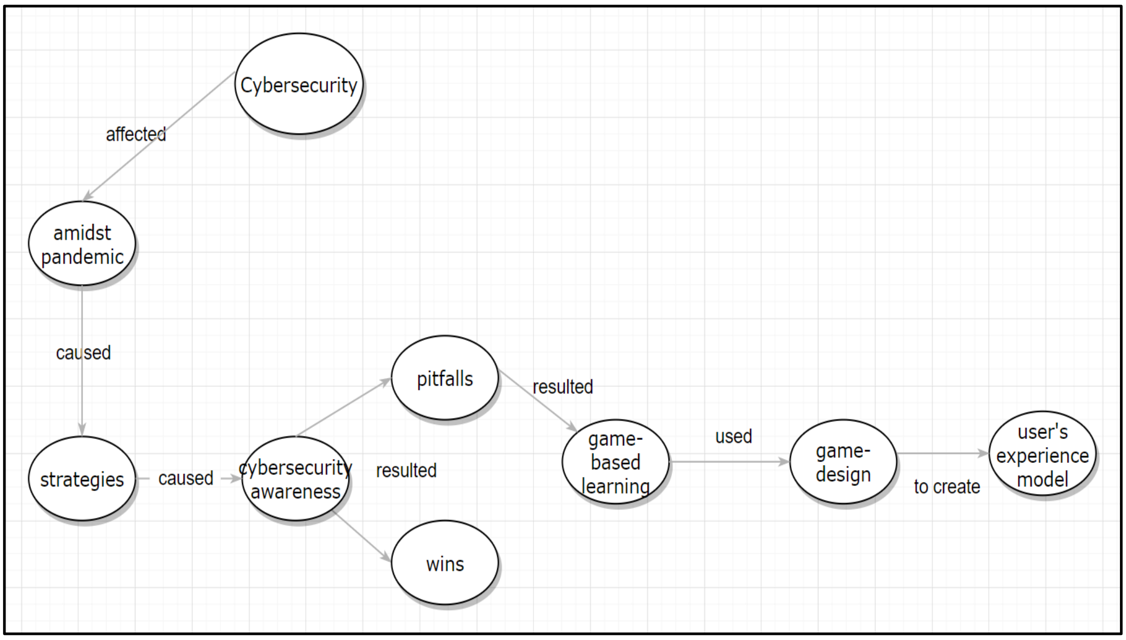

Figure 7. Thematic Analysis

The current setting imposed by the COVID-19 pandemic have accelerated the transformation and highlighted the priorities of the global, regional, country, and agency level management. This is highly evident in EU commission's programs and projects. According to a cybersecurity expert interviewee, international development agencies are reframing their priorities to acknowledge and act upon on the important role of cybersecurity in building and developing society. From an interview with cybersecurity management team leads, EU together with the regional coordinating institution have noticed the effort since 2010 from member states to "ensuring, preventing, and protecting critical national systems against cybersecurity attacks and risks". Both EU cybersecurity management leads noted that the regional institution strongly fosters coordinated and collaborative responses to this threat while ensuring targeted initiatives to various sectors on its member states.

While EU accelerates its initiatives, they are also strengthening various institutions with capacity to increase resilience, and build operational capacity (prevent, and respond). The European Commission that has been setting up legislative framework which strengthens mandates for national competent authorities for various stakeholders and collaboration. These are taken to ensure the organizations' cyber exercise and enhanced preparedness. Parallel to the acceleration of EU initiatives on cybersecurity is the strengthening of various institutions. As result the commission has seen a deliberate development, a strong collaboration among networks of competent authorities to solve and mitigate cybersecurity risks on specific critical systems. Member states are investing on raising awareness to secure home office/ school networks. A coordinated approach is also evident in the running cybersecurity awareness campaigns. ENISA issues materials to raise cybersecurity awareness on the current set-up of working and learning among member states. Sharing good practices among member states became an evident norm in the region.

Technology advancements and sophisticated changing of threats hone the responses and prevention in the greater scheme of things in the digital space. As the technology advances, risk increases to cause a cyberattack and which expands the impact of reach. Certainly, private sectors have taken the driver seat to further the improvements because of the losses (financially and functional) on a cyber breach. Legislation and regulation play a key role to create a conducive environment and reinforce interventions. Adopted way of doing things or the culture of each nation greatly affects the efficiency of various proposed practices and interventions. This also implies change of mind set up to the core to harness improvement.

Even before the remote setting became the only option, Estonia' culture of working-in-a-distance has been adopted in most of the government agencies but medical sector. The only difference now is the number of employees doing this type of set-up and the cloud technologies and remote systems used to ensure the security of the data collected from each end of every government agency. The Information System Authority (RIA) with its Standards and Supervisory division, ensures that government sector and vital service providers are using and following the cyber security standard.

Singapore has experienced upsurge of cyber incidents from 2019. The country heightened its response by supporting organizations in dealing with harmful penetration attempts. With the work from home set-up, Singapore accelerates raising its cybersecurity standards by strengthening the resilience of country's critical infrastructure and improving response cycle to threats and exposed vulnerabilities. Through a cohesive approach with the critical stakeholders, cyber exercises and awareness campaigns are strategically conducted.

Cybersecurity Awareness Initiatives: Wins and Pitfalls

One of the Pillars of the cybersecurity capacity building is the cyber awareness and literacy of the general population. All the participants in the KII who have experience on cybersecurity and capacity building on cyber security agreed the equal importance of the cyber literacy of the citizens to the investments made for better infrastructures and proactive experts. It is deemed as vulnerable and initial touchpoint to a massive blast yet to unravel if not prevented. The pandemic work set-up highlighted the urgent need of investing to the cybersecurity awareness initiatives. Various schemes and platforms are being resorted and tried to harness better results including participatory and multi-stakeholder approach which the deemed helpful in pursuing coordinated and collaborative outcome. Institutions have been utilizing from traditional approaches of chalk and talk, instructor-led, training of trainers, simulation, tabletop, social media campaigns, etc. Many are not scalable but can always identify audience for it.

European Commission's DG CONNECT, ENISA and other critical agencies are working together to improve solutions to reaching out general sector and public sector on cybersecurity awareness. ENISA launched the utilization a diffusion of network approach through ambassadors. This seeks the influence and reach of social media to carry the message on cybersecurity. They are also started adopted the gamification approach in some of the processes and campaigns. A diversified approach is the primary approach taken by EU. The variety of audiences is major consideration before jumping to another platform. To date, social media reach is at its unimaginable rate. Thus, this is being maximized by the EU institutions. It appears the consistent and heightened initiatives of the union, thus, maturity on these is being discussed. A cybersecurity maturity index will be rolled out to measure the progress of a certain nation to ensuring cybersecurity. Competency networks is recently established to create a common hub of experts in the field and use this platform for a community of practice.

[111]:

> "DigiTest helps enhancing citizen's cyber hygiene", this is the recent findings of RIA captured in the Cybersecurity Report 2021. The same report has documented the increase of users' reach with 15,000 public sector employees have accomplished the test. The platform is also a training platform. It comprehensively processes and presents every answer a leaner has given classifying from no risk to high risks actions taken throughout the DigiTest experience or journey.

RIA is targeting the annual use of the training platform and have employees achieve an optimal result. DigiTest does not only act as training platform but also provides rich anonymous data on the profile of the employees and aggregated results on the risk profile of the public sector. The platform also adopted game elements to improve learning experience. The platform has been updated adding more specific cases, and interactive elements. The institution also covers the resources needed to facilitate the use and continual improvement of the systems. Apart from Cyber hygiene test, Estonia regularly implements "prevention and awareness campaigns". There was an immediate shift and add-on in the content of the campaigns to fit the current risk set-up of remote working [111]. The same report has documented the tweak made on the 2019 slogan, "Be IT-conscious" to "Be especially IT-conscious". RIA is on its constant quest to improve the system and create ripples to bigger impacts in the human-aspect of the chain.

Specific experiences captured from an interview with a managerial-level position from an Estonian government agency have brought more empirical data on how learners received the cascaded or rolled-out cybersecurity awareness initiative. According to the public sector officer, cyber hygiene test apart from a yearly recurring training, became part of the onboarding process of the agency. It is a mandatory task for everyone. The public sector official confirmed that the agency adopts a process of which the agency is making sure that every new employee who are on the probation period has accomplished the DigiTest. According to the public sector official, DigiTest has presented conceptual and practical knowledge. The system allows learners to revisit their notes or references. It was also confirmed by the same interviewee how smart and witty the questions were formulated while maintaining that level of challenge.

Cyber awareness in Singapore is evidently captured through the “Go Safe Online” campaign from the overarching masterplan, Singapore’s Safer Cyberspace Masterplan 2020. This is spearheaded by the Cybersecurity Agency of Singapore supported by various alliances.

[68]:

> The country also targeted to create an “Internet Cyber Hygiene portal” along with the constant innovations to enhance awareness of the states’ “cyber-savvy population”. Singapore transparently indicated in the master plan report that “more than 4 out of 10” nationals are struggled to correctly spot a strong credentials or passwords. While 4% can identify seamlessly phishing emails.

Other relevant rate on adoption and attitudes of Singaporeans are also captured in the 2020 cyberspace masterplan. Having a results-based starting-point, Singapore started to create tool kits. The website of “Go safe Online” provides an array of tool kits that are adaptable to various organizations including public sector. Cybersecurity campaigns are embodied in (1) Cyber Safety Interactive Handbook; (2) Incident Response Checklist; (3) Online password checker (“Password Café”); (4) Employee Cyber Security Kit, etc. Singapore adopts a collective responsibility or what they called “community-centric approach” [68]. Community champions or the “cyber-savvy” members of the community act as a multiplier by sharing knowledge on how to protect ourselves. It can be among your work colleagues, friends, or family members. To infuse learning while having fun in the strategy, Singapore has already started adopting “interactive games” to empower public to learn cybersecurity. An important strategy mentioned by government officer from CSA is the changing of mindset continuously. Clear understanding of importance of the securing the cyber space should be instilled up to the core country’s citizens.

While we celebrate and recognize the road to a win-state, pitfalls are here to stay to improve implementation schemes. Participants in KII identified various hurdles that are yet to be managed. Awareness and education in EU have been implemented to increase knowledge and practical-know-how, measuring the increase or impact of this initiative is challenging considering each member state's individual initiative. Pool of security skills in the region is always difficult to get hold of. Available experts usually stay with private sectors. For the initiatives of EU as a region, limited funding is becoming a key consideration every inception of a project or program. Estonia is working on the harmonization of various platforms for the cyber hygiene test. Other ministries took the autonomy of developing their own platform. While the unifying these tools is the way froward, behaviour change of its citizens is the end goal. Singapore is dealing with solutions to accelerate the instilling of security mindset among public sector and private organizations.

Game Design towards Win-State

Certainly, perception on games have evolved from merely a "play" to a "strategic platform" for learning this is evident with the discussion with game-based practitioners from Academe and International development organization. It was noted from 11 out 11participants in the interview the feasibility of integrating games to most fields, if not all. But still, game-based practitioner from a University in Estonia emphasized that it will always be a point of argument if games would be the only best way of transmitting information. Though perceptions have evolved from play perspective, game-based practitioners agreed the limited understanding of the method. Both have agreed that many of the target users understand the word "game" connotes fun which suggest least optimization of learning and can never be combined with more real-life related tasks. Thus, the word "serious" in the Serious Games.

Game-based practitioners have both confirmed the capacity of game to provide an environment that provides "opportunity to learn from mistakes" or shortcoming without having real-life implications. It is deemed as a "safe place" for failure where one can apply the knowledge and verify how its work around. UNESCO MGIEP have adopted Games for Learning on its several projects and courses. The institution is integrating games in major initiatives such as development of games for SDG's and learning courses on social and emotional learning courses. Two (2) games were developed under this portfolio (World rescue on sustainable development and Cantor's World on nations and economy). The initial strategy was to develop games directly spearheaded by the institution which also included hackathons. UNESCO eventually realized that producing original games will take resources (time, expertise, funds). These considerations became a significant turning point in the next decision the institution have taken.

The Institution started to evaluate online games available in the market. They paid for the licenses for some, made membership in various gaming sites, brought gaming console in the office to try out these games. Group of six (6) on the age group of 20-30 years old. They have evaluated a long list using the parameters of they have set parameters in evaluating, (1) narrative-based story, characters, and non-violent games. They came up with short-list, then started to play the game and shared notes, what overlapped and contradicted from one evaluator to another. They came up with draft list of things a learner could learned from the game. After which, they held a co-design workshop with the target users of the game, K-12. They asked the students to do the same process as what they did, play the games and identify what did they learn from it. Those learning that overlapped with what they have drafted was the critical indicator of the potential of these games in teaching certain subject matter.

The process did not only end with the student, but UNESCO MGIEP also reached out to students, they have extended it to teachers and parents. They asked teachers to play the game and derive what they could use to teach students in social and emotional learning. They initially had to deal with teachers who have seen games as a play instead of an effective learning process. Most teachers, if not all, became passionate about the game solution in place after a thorough discussion how even them learned a lot from games (unconsciously). Eventually, games that made into the list were rolled out in the courses of social and emotional learning and made available to students. Pre and post assessment tools were implemented to measure the learning of the 600 students, controlled and experiment group. Massive increase of knowledge was recorded from the conduct of assessment. UNESCO MGIEP was able to manage to embed social and emotional learning on their courses which made the entire learning journey engaging and fun while ensuring optimal learning.

The evaluation UNESCO MGIEP made for various games they assessed turned into gaming design guidelines was also shared among the gaming development industry. They are using these findings to influence gaming design. Most of the companies they have talked to did not realize they have developed something that can be used in teaching social and emotional learning. These companies are always fascinated how those games they have developed originally intended for entertainment can be used to teach. UNESCO MGIEP deliberately opens more avenues for conscious game design. To date, UNSECO MGIEP works with i-Thrive, a New York based organization, on developing ways on how to maximize games for learning.

EU Joint Research Center (JRC) has also implemented a game-based learning for GDPR, K-12 as the primary targets. Cyber Chronix was launched in 2017subsequesnt to the introduction of GDPR. This game came after the launched of Happy onlife. Cyber Chronix follows a digital comic strip with storytelling branches [112]. The game came to life using a participatory approach among target K-12 users. EU JRC recognizes the importance of digital competences to enhance strategies on privacy. Consultation with users is highly valued as the EU JRC fosters participatory approach in creating solutions.

Specific game elements were also identified in the process from experts and game-implementation experienced participants of the KII. The following emerged as dominant gaming elements:

- Story driven
- Relatedness of players- sense of community/ learners with the characters presented
- Vocabulary reference as knowledge component
- Incentives instead of punishment
- Sense of healthy competition (compete with time)
- Progress board
- Rewards
- Calling for a meaningful task
- Historical references-relatedness
- Balance between skills and challenge
- Immediate feedback or debriefing after the game play

According to one of game-based practitioners, debriefing after the game play is critical aspect of learning using game. This can be included in the game can be done as process of learning. This processes learning (what did you learn, what happened in the game, etc.). Games like any other digital solution is not an absolute intervention. Users and learners are always key consideration in building a game design. Designers differentiate players by their demographic (e.g., age, gender), and psychographics (attitudes, opinions, behaviours, etc.).

In many of the known explorations for games for learning, experts have noted how initial implementation just gone with the wind or remained to be at pilot phase because, mainly, of funding issues and other resource constraints. Evidently, games are time consuming to create, need expertise to consciously embed game designs which are helpful for learning, and require funds to keep it running. Some of the games searched on the internet for the evaluation described previous in methodology were shutdown, initial development was not followed through, or just not anymore available. UNESCO MGIEP approach of maximizing whatever is available in the market plays a critical role in solving the funding resources issue.

Games is thriving. ENISA, RIA, eGA, and CSA are exploring the use of variety of strategies and testing solutions such as game-based learning as viable option in building and strengthening cybersecurity awareness initiatives of respective organizations. Resources of not only funding but experts are dominant hurdles in adopting games as delivery method. Cybersecurity awareness can slowly embed the game-based learning/ elements by adding modules in the learning process like what UNESCO MGIEP did.

4.3 RQ 3: Target Learners

Initially, two (2) public sector agencies were identified and invited for the FGD. Both confirmed to participate. However, towards the schedule of FGD, one of which decided to decline the invitation because of the perception that the organization does not have that much experience on the subject matter, thus, might not of help in the process of the study. The present thesis also sought other organizations but have not received confirmation or any response. The study pursued the methodology for a systematic inquiry to the end users of the proposed platform.

According to the interview with public officer, Social Insurance Board is nearly 700 employees serving 700,000 clients. The public sector provides 30 public services such as pension benefits, rehabilitation benefits, services for persons with disability, childbirth benefits, etc. Basically, the Social Insurance Board holds delicate individual-level of information from the clients. Four (4) participants have confirmed. Social Insurance Board government officer who also participated in the KII helped the present study to identify strategic participants in the discussion.

The FGD used MS teams to record the proceeding and Google jamboard to facilitate the discussion. Participants were asked to share their thoughts and experiences on cybersecurity awareness they have experienced with the present agency. Through the collaborative Participants represent various age group from 25-30 years of age, 31-40 years of age, 41-50 years of age, and 51-55 years of age. All have been employed in the insurance board for an average of 12.5 months. They are representing various units of the office, namely, accessibility, digital/ innovative solutions, preservation, and business requirement units. Apart from work, the participants are involved in various personal activities (outdoor activities, travel, and family) of which they have devoted their time with after work.

Participants defined the cybersecurity as an integral function which allows the data used and sharing secured from unauthorized access. One of the participants suggested the element of good cyber hygiene to achieve a secure cyber space. Two of the participants mentioned how cybersecurity increase the trust in the digital world. According to one interviewee, cybersecurity also involves legal obligation when a cyber breach occurred. All the participants recognize the importance to ensure the cybersecurity which leads to data protection and securing the functions of the organization. A well-founded understanding and recognition of the role of cybersecurity in the organization opens more opportunity for discussion to improve or attain certain state of security.

All the participants have accomplished the DigiTest as a compliance to their onboarding procedure. Since it is a mandatory task, no one is exempted. A strict deadline was also followed to ensure the timely accomplishment of the task. Participants accomplished the test in the workplace. All the participants agreed that the DigiTest is simple, straightforward, and has intuitive process which makes the system easy to navigate. One of the participants found the process a bit monotonous but still manage to ignite interest towards the system. The platform presented videos, and multiple choice. One of the participants noted the probability of misinterpreting the given questions, thus, it is not something enjoyable to do. While another participant has another of impression of the system. For this participant, the system provides clear instructions, and all the subjects are easy to grasp.

The evident goal of the learners while using the system is to pass a certain threshold of learning as set by the system. All the participants got particularly good results. One did not even need to study further the materials provided to get a passing mark. One participant recognizes the learning the test is trying to transmit to the learners. The system allows learner to repeat the examination which allows learners to commit mistake in the process and eventually correct what have been learned. Arriving to the preferred state, passing at the very least, made the learner feel fulfilled and happy after taking the test. However, one participant realized the need to create another level of learning after finishing the standard test. Because they have been the taking the same set for questions for quite sometimes.

2 out of 5 of the participants explicitly said that they have not yet used any of the learning they have acquired in daily work or workplace. One of the participants is more cautious on suspicious email. One participant shared his experience of that one of the co-workers refuse to participate of the fear that the information might be shared with unauthorized access. 100% of the participants are feeling highly confident with the acquired skills on cybersecurity awareness topics. It is also evident with their responses that the confidence mainly originated with their experiences. To reinforce and sustain the level of confidence, participants thought of the following intervention:

- More thorough training
  - variation on the manner the topics are being presented
  - option of upgrading one’s learning by having a next level test with an increase difficulty after mastering basic level
  - regular practical training with simulated set-up
- Community of Practice that can efficiently facilitate sharing of best practices and common knowledge

3 out of the 4 participants have tried playing an online game. However, one of those who have played the game had the last one 15 years ago. Two of the participants played the game because they find it fun and enjoyable when done with friends. One of the participants find games as training for strategy which helps them to refresh their mind with another perspective.

The participants shared their views and insights on how games can be incorporated in the cybersecurity awareness training/ test they are having now. All agreed for a realistic/ practice tasks or a simulation set-up. 2 out of 4 participants value the achievement of getting high score or less to no mistakes in the journey of learning. One participant sees competition as possible option for those who are competitive and wants to show their rating. Good jokes or fun way of presenting the topic with aesthetically graphics were the things one of the participants suggested to encourage learners to use the system. However, they also seen risk that can surely occur ahead of implementation. There would be people who have less to none gaming experience that would comprise those who might be strongly reluctant to use the platform. Apart from the limited experience, there would be population who see game as not acceptable platform for learning.

On the other hand, one participant sees those who are into games might not take the process as learning but rather only fun. To improve or mitigate the foreseeable challenges participants identified support needed to sustain their use of a game-based cybersecurity awareness platform, to wit, (1) clear instructions with interactive process; (2) excitingly adventurous enough to ignite more curiosity and competitiveness; (3) progress of learning to encourage learning; (4) bonus tracks that may allow learner to take shorter route.

Evidently, the participants of the FGD presents various elements that can motivate learners on a game-based platform. Most of the cybersecurity awareness initiatives are designed as mandatory training among public sector in Estonia, core drive to adopt for learners would be a meaningful call for action and challenge. For Onboarding phase, learners can easily be engaged by utilizing Ownership and Possession motivational core drive. Adopting game elements which allow the learners to create their own character in the game. Another option would be including Social Influence and Relatedness by adding a feature of which learners will be able to discuss, share, and interact with other learners in the game as they try to get onboard. Progress board or Accomplishment and Development core drive was also identified as motivational element in the game to monitor own progress.

Game element on Social Influence and Relatedness is suggested to be kept through the learner’s journey to continuously engage with community of practice. This is also explicitly determined by game-based practitioners and experts to sustain the interaction in the learning process. It is also important to add Empowerment and Feedback in every task accomplishment to immediately process the learning and be put into context. A comprehensive processing of the learning can be done by adding debriefing every after milestone. This can be done in a forum built in the game. Everything that has been done in the game will be out into a context of which beneficial in real-life related circumstance. As the platform is a safe space, Unpredictability and Curiosity on possible outcome of the learning experience can be ignited if the challenge can be repeated.

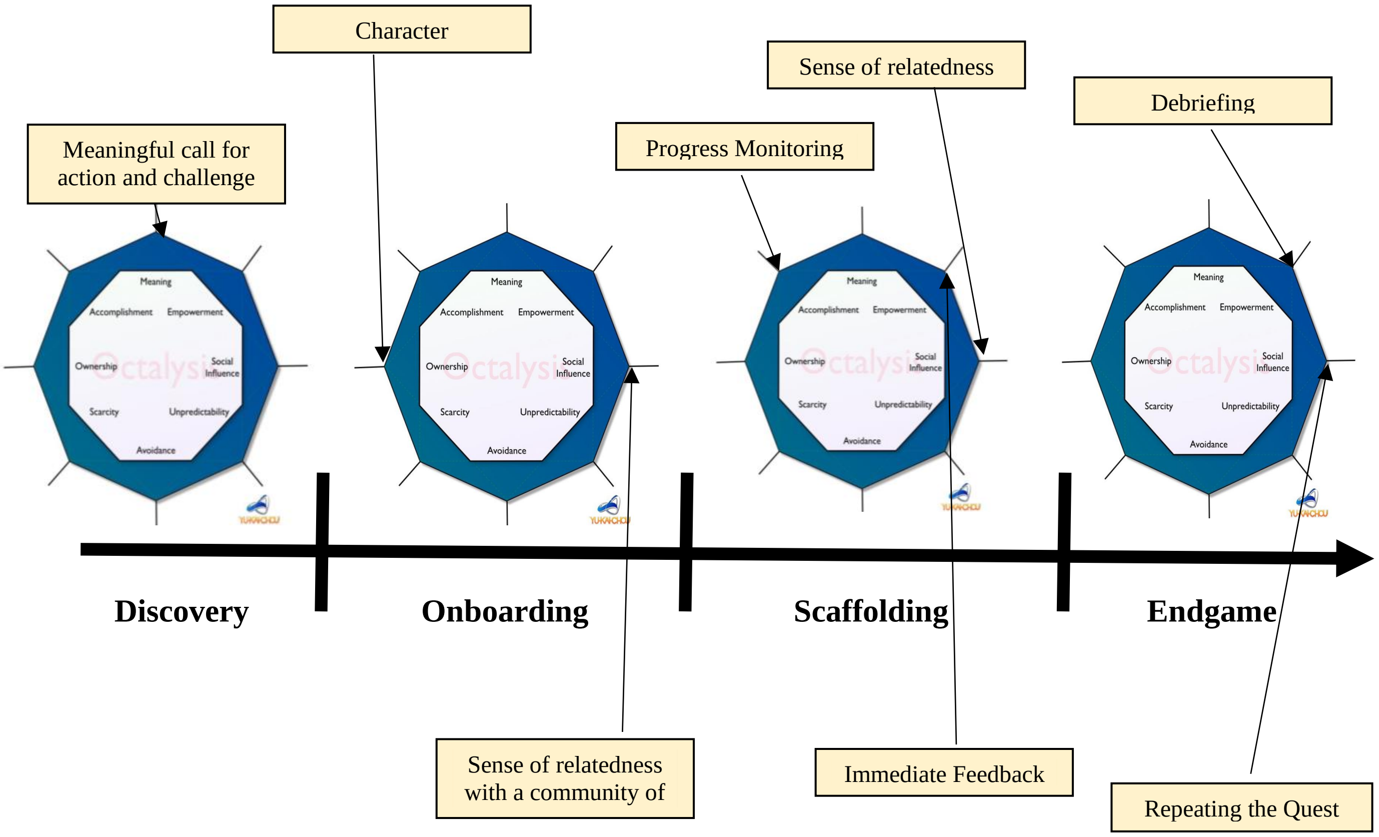

Figure 8. Proposed User's Experience Model

5 Limitation and Future Work

The present study limits its scope on the integration of the game-based learning to cybersecurity awareness, specifically, with the framework on motivational core drives, and users' journey. It primarily sought to identify the motivational core drives of game-based learning, preferred users' journey while understanding the current landscape of the cybersecurity and initiatives utilized to date. The approach is limited to free and popular game options online. FGD was conducted with limited focus group. The author suggests an expanded search including paid versions of games and sites which require membership. The same process adopted by UNESCO MGIEP is highly recommended. Inquiry to the other learners is highly recommended to be expanded by including other public sector agencies but not limited to organizations that are handling sensitive and individual-level data. It is relevant to understand the insights from those organization which see themselves as low target because of the low-risk data they are working on. Benchmark of the initial level of learning should also be measured to available data on the actual use of the game-based to compare the level of learning.

6 Conclusion

The present study has presented various data from three (3) approaches, assessing online cybersecurity games, data gathering from expertise and experienced key informant interviews, and specific experience and recommendation from the users of the system. Specifically, the study has answered the research questions:

RQ 1: How do online games for cybersecurity awareness position its core motivational drivers?

Evaluated cybersecurity online games have presented motivational core drives found on various game-elements which are position in the phases of the game (Onboarding, Scaffolding, and Endgame). These core drives classified as white/ black hat and extrinsic/ intrinsic motivations that can only be as effective and motivational if used strategically while complimenting other core drives based on the targeted learning experience of the learners. Accessible cybersecurity games found online posed opportunity to significantly affect the learning and learning experience of the learners by providing practical knowledge and realistic tasks to learners based while reinforcing the motivation of the learners with core drives strategically in place in the learner's journey. The results and processes done are recommended to be adopted by public sector or an organization drafting cybersecurity awareness initiatives with game-based learning as platform. The result of the assessment is highly recommended to the lead implementors in the cybersecurity awareness initiatives who are currently exploring for a game-based learning approach for cybersecurity. Free games can always be added in the module to gradually integrate the game-based learning in the current process.

RQ 2: How can game-based learning be integrated into the cybersecurity awareness capacity building approach for the public sector?

Resources in the form of expertise, time, and funding have presented impact on the course of action towards the use of game-based learning. This is evident to those games made in the past but were not sustained due to funding availability and remained to be at pilot scale.

However, with the captured experience of UNESCO on the maximizing already available resources is a game-changer. It presented a critical consideration on what existing online games can contribute on the targeted learning and learning experience. With thorough review and adoption of collaborative approach with learners and other experts, limited resources are not an endgame on its own. Decision-makers on the platform used in the cybersecurity awareness. Founded game-based elements which coincide with the motivational core drives as recommended by the experts and practitioners will bring the game design to optimization of learning and sustaining learning experience of the learners. Public sector or an organization highly considering the use of another viable option such as game-based learning should learn from the experience of UNESCO MGIEP. Decision makers or cybersecurity capacity building lead or top management may use the findings to further the search of possible option of game-based learning approach in cybersecurity awareness implementation.

RQ 3: How can game-based learning improve learning and learning experience in the cybersecurity awareness training?

Motivational drives of the learners of the system were sought to further understand critical factors that would sustain the use of the system. The identified elements are evidently found in the Octalysis Framework. Certainly, it presented how the framework and preferred learner experience coincide. Perspective from the learners will always be at forefront in designing the entire learning experience for their use. Findings and data gathered from target learners are most valuable to influence conscious game design for games founded to build and strengthen cybersecurity awareness. Game industry may use the result to improve game design and consciously target motivation and learning at the same time. The study would also be beneficial to public sector or an organization which attempting to understand its user’s behavioural motivation.

References

[1] A. Ott, "Foreword," in *National Cyber Security in Practice*, Tallinn, e-Governance Academy, 2020, p. 5.

[2] MEAC, "Cybersecurity Strategy," Ministry of Economic Affairs and Communications, Tallinn, 2018.

[3] A. Kasper, "Time for Cyber Maastricht," 15 November 2020. [Online]. Available: https://directionsblog.eu/time-for-cyber-maastricht/.

[4] European Union, Cybersecurity Act, "Cybersecurity Act," 17 April 2019. [Online]. Available: Cybersecurity Act (Article 2).

[5] J. Vseviov, "Tallinn Winter School of Cyber Diplomacy, 2021," in *Tallinn Winter School of Cyber Diplomacy, 2021*, Tallinn, 2021.

[6] INTERPOL, "News and Events," 4 August 2020. [Online]. Available: https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-shows-alarming-rate-of-cyberattacks-during-COVID-19.

[7] F. Alotaibi, S. Furnell, I. Stengel and M. Papadaki, "A Review of Using technology for Cyber- Security Awareness," *International Journal for Information Security Research,* vol. 6, no. 2, pp. 660-666, 2016.

[8] eGovernanceAcademy, "NCSI," eGovernance Academy, 28 February 2020. [Online]. Available: https://ncsi.ega.ee/country/ee/. [Accessed 16 September 2020].

[9] e-estonia, "e-estonia," 2020. [Online]. Available: https://e-estonia.com/.

[10] M. Hendrix, A. Al-Sherbaz and B. Victoria, "Game based cyber security training: are serious game suitable for cyber security training?," *International Journal of Serious Games,* vol. 3, no. 1, pp. 53-61, 2016.

[11] T. Anastasiadis, G. Lampropoulos and K. Siakas, "Digital Game-based Learning and Serious Games in Education," *International Journal of Advances in Scientific Research and Engineering,* vol. 4, no. 12, pp. 139-144, December 2018.

[12] J. Bhardwaj, Design of a Game for Cybersecurity Awareness, North Dakota State University, 2019.

[13] L. Carter and F. Belanger, "The utilization of e-government services: citizen trust, innovation and acceptance factors," *Information Systems Journal,* pp. 5-25, 2005.

[14] M. Kianpour, S. J. Kowalski, E. Zoto, C. Frantz and O. Harald, "Designing Serious Games for Cyber Ranges: A Socio-technical Approach," in *2019 IEEE European Symposium Security and Privacy Workshops (EuroS&PW),* 2019.

[15] European Commission, "Shaping Europe's digital future: Cybersecurity Policies," 26 March 2021. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies.

[16] L. Chang and N. Coppel, "Building Cyber Security Awareness in a Developing Country: Lessons of Myanmar," *Computers and Security Journal,* pp. 44-57, 2019.

[17] Cyentia Institute, "IRIS 20/20 Extreme: Information Risk Insights Study," Cyentia Institute, Florida, 2020.

[18] H. deBruijin and M. Janssen, "Building cybersecurity awareness: The need for evidence-based framing strategies," *Government Information Quarterly,* pp. 1-7, 2017.

[19] J. Zhao, S. Zhao and S. Zhao, "Opportunities and threats: A security assessment of state e-government websites," *Government Information Quarterly,* pp. 49-56, 2010.

[20] ENISA, "Main incidents in the EU and worldwide," ENISA, Attiki, 2020.

[21] Trend Micro, "Report on cybersecurity and critical infrastructure in the Americas," Tren Micro, 2016.

[22] J. Abawajy, "User Preference of Cybersecurity Awareness Delivery Methods," *Behaviour and Information Technology,* pp. 237-248, 2014.

[23] ENISA, "List of top 15 threats," 20 October 2020. [Online]. Available: https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends#:~:text=The%20European%20Union%20Agency%20for%20Cybersecurity%20(ENISA),%20with,January%202019-April%202020.%20Infographic%20-%20Top%2015%20Threats.

[24] ENISA Threat Landscape, "List of Top 15 Threats," ENISA, Attiki, 2020.

[25] H. Kettani and P. Wainwright, "On the Top Threats to Cyber Systems," *IEEE 2nd International Conference on Information and Compuer Technologies,* pp. 175- 179, 2019.

[26] S. Venkatachary, J. Prasad and R. Samikannu, "Economic IMpacts of Cyber Security in Energy Sector: A Review," *International Journal of Energy Economics and Policy,* pp. 250-262, 2017.

[27] Z. Malekos-Smith and E. Lostri, "The Hidden Costs of Cybercrime," Center for Strategic and International Studies (CSIS), Washington DC, 2020.

[28] D. Eade, Capacity-Building: An Approach to People-Centered Development, Oxford: Oxfam GB, 1997.

[29] S. eds Kenny and C. Matthew, Challenging Capacity Building: Comparatove Perspectives, Hampshire: Pagrave Macmillan, 2010.

[30] Z. Homburger, "The Necessity and Pitfall of Cybersecurity Capacity BUilding for Norm Development in Cyberspace," *Global Society,* pp. 224-242, 2019.

[31] W. Dutton, S. Creese, R. Shillair and M. Bada, "Cybersecurity Capacity: Does It Matter?," *Journal of Information Policy,* pp. 280-306, 2019.

[32] Oxford Martin School, "Global Cyber Security Capacity Centre," 2021. [Online]. Available: https://gcscc.ox.ac.uk/the-cmm#/.

[33] W. Dutton, S. Creese, R. Shillair and M. Bada, "Cybersecurity: Does it matter?," *Journal of Information Policy, Vol 9,* pp. 280-306, 2019.

[34] World Economic Forum, "The Global Risks Report 2017: 12th edition insight report," World Econmic Forum, Geneva, 2017.

[35] EU Institute for Security Studies, "Capacity Building in cybersapce: taking stock," European Union, Brussels, 2013.

[36] ENISA, "European CyberSecurity Month," European Union Agency for CYbersecurity, 2021.

[37] ENISA, "ENISA and CERT-EU sign Agreement to start their Structured Cooperation," 2 March 2021. [Online]. Available: https://www.enisa.europa.eu/news/enisa-news/enisa-and-cert-eu-sign-agreement-to-start-their-structured-cooperation.

[38] CCDOE, "Training," January 2018. [Online]. Available: https://ccdcoe.org/training/.

[39] European Commission, "EUROPE 2020: A strategy for smart, sustainable, and inclusive growth," European Commission, Brussels, 2010.

[40] J. Munoz-Castano, C. Redecker, R. Vourikari and Y. Punie, "Open Eductaion 2030: planning the future of adult learning in Europe," *Open LearningL The Journal of Open, Distance and e-Learning,* pp. 171-186, 2014.

[41] European Centre for the Development of Vocational Training, "Validation of non-formal and informal learning," 2014. [Online]. Available: https://www.cedefop.europa.eu/en/events-and-projects/projects/validation-non-formal-and-informal-learning/european-inventory/european-inventory-glossary#l.

[42] European Commission, "European Commission," 2013. [Online]. Available: http://ec.europa.eu/education/lifelong-learning-policy/adult_en.htm.

[43] C. B. Tweedell, "A Theory of Adult Learning and Implications for Practice," in *Annual Meeting of the Midwest Educational Research Association*, Illinois, 2000.

[44] J. Collins, "Education Techniques for Lifelong Learning," *Lieflong Learning,* pp. 1483-1489, 2004.

[45] S. Lieb, "Principles of Adult Learning," pp. 1-8, 1991.

[46] C. Widick, P. Clyde and L. Knefelkamp, "Erik Erikson and Psychosocial Development," *New Directiosn for Student Services,* pp. 1-17, 1978.

[47] J. Heckhausen, C. Wrosch and R. Schulz, "A motivational theory of life-span development," *Psychological Review,* pp. 32-60, 2010.

[48] J. D. Bransford, A. Brown and R. Cocking, "How People learn: Brain, mind, experience, and school," *National Academic Press,* 2000.

[49] J. Eyler, "The Power of Experiental Education," *Liberal Education Fall 2009,* pp. 24-31, 2009.

[50] E. L. Deci and R. M. & Ryan, "Self Determination Theory," in *Handbook of Theories of Social Psychology: Volume 1,* SAGE Publications Ltd, 2012, pp. 416-436.

[51] L. Chang and P. Grabosky, "The Governance of Cyberspace," in *Regulatory Theory: The Governce of CYberspace,* Canberra, ANU Press, 2017, pp. 533-551.

[52] M. Bada, A. Sasse and J. Nurse, "Cybersecurity Awareness Campaigns: Why do they fail to change Behaviour," *International Conference on Cybersecurity for Sustainable Society,* 2015.

[53] N. Davinson and E. Sillence, "It won't happen to me: Promoting secure behaviour among internet users," *Computers in Human Behavior*, pp. 1739-1747, 2010.

[54] Wilson, M; Hash, J, "NIST: Building an Information Technology Security Awareness," National Institute of Standards and Technology: Computer Security Division Information Technology Laboratory, 2003.

[55] Z. Yunos, R. Ab-Hamid and M. Ahmad, "Development of a Cybersecurity Awareness Strategy using Focus Groud Discussion," *2016 SAI Computing Conference*, pp. 1063-1067, 2016.

[56] R. Shaw, "The impact of information richness on information security awareness training effectiveness," *Computers and Education Vol 52 (1)*, pp. 92-100 , 2009.

[57] Coventry, Lynne; Briggs, Pam; Blythe, John; Tran, Minh, "Using behavioural insights toimprove the public's use ofcyber security best practices," Government Office for Science, Gov. UK report, London, 2017.

[58] A. Nagarajan, J. M. Allbeck, A. Sood and T. Janssen, "Exploring Game Design for Cybersecurity Training," in *IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems*, Bangkok, 2012.

[59] B. Cone, "A video game for cybersecurity training and awareness," *Computers and Security*, 2007.

[60] L. Anneta, "The "I's" Have It: A Framework for Serious Educational Game Design," *Review of General Psychology Vol 12 Issue 2*, pp. 105-113, 2010.

[61] D. Kolb, Experiential Learning: Experience as the Source of Learning and Development, New Jersey: Prentice Hall, 1984.

[62] M. Barzelay, "Chapter 1. Encountering design-oriented public management," in *A Design-oriented Professional Discipline*, Massachusetts, Edward Elgar Publishing, Inc, 2019.

[63] S. Dawes and C. M. E, "Intergovernmental Digital Government through G2G Relationship and Applications," *Encyclopedia of Digital Government Vol 5*, pp. 1114-1119, 2007.

[64] A. Baležentis and G. Žemaitaitienė, "The Benchmarking of the Government to Employee (G2e) Technology Development: Theoretical Aspects of the Model Construction," *Social Technologies Vol 2 No 1*, pp. 53-56, 2013.

[65] H. Tang, "Using Association Rules Mining to Provide Personalized Information in E-Government," *Internationa Conference in e-Business and e-Govenrment (ICEE) in China*, 2011.

[66] A. Golubeva and I. Merkuryeva, "Demand for online government services: Case studies from St. Petersburg," *Information Polity 11,* pp. 241-254, 2006.

[67] Information System Authority, "Cyber Security in Estonia 2021," RIA, Tallinn, 2021.

[68] Cybersecurity Agency Singapore, "Singapore's Safer Cyberspace Masterplan 2020," Cybersecurity Agency Singapore, Singapore, 2020.

[69] T. Laning, "Serious games, gamification, and game-based learning: what's the difference?," 2018. [Online]. Available: https://grendelgames.com/serious-games-gamification-and-game-based-learning-whats-the-difference/.

[70] D. Crookall, "Serious Games, Debriefing, and Simulation/ Gaming as a Discipline," *Simultion and Gaming, Sage Publications,* pp. 898-920, 2010.

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

[72] Y.-k. Chou, Actionable Gamification, CreateSpace Independent Publishing Platform, 2014-2015.

[73] M. Csikszentmihalyi, S. Abuhamdeh and J. Nakamura, Flow: Flow and the Foundations of Positive Psychology, Springer, Dordrecht, 2014.

[74] E. Boyle, T. Connolly and T. Hainey, "The role of psychology in understanding the impact of computer games," *Entertainment Computing,* pp. 69-74, 2011.

[75] N. Lazzaro, The 4 Keys to Fun: Increasing Engagement with Games, XEO Design, Inc IBM, 2013.

[76] N. Eyal, Hooked: How to Build Habit-Forming Products, Penguin Random House, 2014.

[77] K. Becker, "A Magic Bullet for Assessing Games for Learning," in *Teacher Education International Conference*, 2012.

[78] UNESCO, "Games for Learning," 2017. [Online]. Available: https://mgiep.unesco.org/games-for-learning-old-page.

[79] I. Mergel, A. Kleibrink and J. Sorvik, "Open Data Outcomes: U.S. cities between product and process innovation," *Government Information Quarterly,* pp. 622-632, 2018.

[80] M. Hernandez and J. Moreno, "A Systematic Literature Review on Organizational Training Using Game-Based Learning," *Communications in Computer and Information Science,* vol. 847, pp. 1-18, 2019.

[81] L. e.dGiven, The SAGE Encyclopedia of Qualitative Research Methods, SAGE Publications, 2008.

[82] D. Thomas, "A General Inductive Approach for Analyzing Qualitatibve Evaluation Data," *American Journal of Evaluation,* pp. 237-246, 2006.

[83] R. Schutt, "Qualitative Data Analysis," in *Investigating Social World*, Boston, SAGE Publications, 2018, pp. 320-357.

[84] K. O'Reilly, Inductive and Deductive In: Key Concepte in Ethnography, London: SAGE Publications Ltd, 2012.

[85] F. Znaniecki, The Method of Sociology, New York: Farrar & Rinehart, 1934.

[86] S. Khan, "Qualitative Research Method: Grounded Theory," *International Journal of Business and Management,* pp. 224-233, 2014.

[87] L. Palinkas, S. Horwitz, C. Green, J. Wisdom, N. Duan and K. Hoagwood, "Purposeful Sampling for Qualitative Data Collection and Analysis in Mixed Method Implementation Research," *PubMed: Administration and policy in mental health,* 2013.

[88] R. Bartle, Designing Virtual Worlds, New York: New Riders Publishing, 2004.

[89] Y.-k. Chou, "Gamification and Behavioral Design," 2015. [Online]. Available: https://yukaichou.com/gamification-examples/octalysis-complete-gamification-framework/.

[90] D. Preuveneers ed, "Evaluation of a dynamic role-playing platform for simulations based on Octalysis gamification framework," in *Workshop Proceedings of the 11th International Conference on Intelligent Environments,* Amsterdam, 2015.

[91] B. Hennessey, S. Moran, B. Altringer and T. M. Amabile, "Extrinsic and Intrinsic Motivation," *Wiley Encyclopedoa of Management,* 2015.

[92] R. Toasa, E. Celi and L. Herrera, "Using accomplishment from Octalysis Framework in a Dynamic Game," in *2020 15th Iberian Conference on Information Systems and Technologies (CISTI),* Seville, 2020.

[93] S. Yudhoatmojo and R. & Ramadana, "Analysis on Gamificaiton Features Usage on Indonesia e-Commerce Sites using Octalysis Framework," in *The 2nd International HCI and UX Conference,* Jakarta, 2016.

[94] D. Tobing, E. Utami and H. Fatta, "Analysis of Dominants Game Elements Using the Sillaots Parameters and Octalysis Framework on the Google Play Store," in *4th*

International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 2019.

[95] C. Teddlie and F. Yu, "Mixed Methods Sampling: A Typology With Examples," *Journal of Mixed Methods Research V1, No 1,* pp. 77-100, 2007.

[96] A. Tashakkori and C. Teddlie, "The past and future of Mixed Methods Research," in *Handbook of mixed methods in social and behavioral research,* CA, Sage, 2003, pp. 671-702.

[97] J. Creswell and D. Creswell, "Collecting Data in Mixed Methods," in *Research Design*, Nebraska, SAGE Publication, Inc., 2009, pp. 203-228.

[98] C. Cohen D, "Stratified Purposeful Sampling," April 2006. [Online]. Available: http://www.qualres.org/HomeStra-3813.html.

[99] Microsoft, "Stream," 2021. [Online]. Available: https://docs.microsoft.com/en-us/stream/overview.

[100] Microsoft, "Microsoft Stream transcript VTT file cleaner," 2021. [Online]. Available: https://web.microsoftstream.com/VTTCleaner/CleanVTT.html.

[101] U. Flick, The SAGE Handbook of Qualitative Data Analysis, London: SAGE Publications Ltd, 2014.

[102] M. Sillaots, T. Jesmin and A. Rinde, "Survey for Mapping Game Elements," pp. 1-10, 2016.

[103] P. Bazeley and K. Jackson, Qualitative Data Analysis with NVivo, Los Angeles: SAGE Publications, 2013.

[104] V. Braun and V. Clarke, "Using Thematic Analysis in psychology," *Qualitative Research in Psychology,* pp. 77-101, 2006.

[105] Trend Micro Incorporated, "Targeted Attack," 2015. [Online]. Available: http://targetedattacks.trendmicro.com/about-the-game.html.

[106] Texas A&M University, "Keep Tradition Secure," 2017. [Online]. Available: https://keeptraditionsecure.tamu.edu/.

[107] Defense Counterintelligence and Security Agency, "Center for Development and Security Execellence," [Online]. Available: https://www.cdse.edu/resources/games.html.

[108] Centrigade, "Cybersecurity Training Through Serious Games," [Online]. Available: https://www.centigrade.de/en/references/cyber-security-training-serious-games.

[109] Naval Postgraduate School, "CyberCiege," [Online]. Available: https://nps.edu/web/c3o/cyberciege.

[110] Cybersecurity Challenge UK, "Cyber Security Challenge UK," [Online]. Available: https://cybergamesuk.com/cyber-city.

[111] Riigi Infosüsteemi Amet, "Cyber Security in Estonia 2021," Information System Authority-Estonia, Tallinn, 2021.

[112] R. DiGioia, S. Chaudron, M. Gemo and I. Sanchez, "Cyber Chronix, Participatpry Research Approach to Develop and Evalaute a Storytelling Game on Personal Data Protection Rights and Privacy Risk," *GALA,* no. LNCS 11899, pp. 221-230, 2019.

[113] "The Design Exchange," 09 Septmber 2017. [Online]. Available: https://www.thedesignexchange.org/design_methods/74.

[114] Y.-k. Chou, "Yu-kai Chou: Gamification and Behavioral Design," 2015. [Online]. Available: https://yukaichou.com/gamification-study/user-types-gamified-systems/.

[115] R. Iris, "Systematically Applying Gamification to Cyber Security Awareness Trainings: A framework and case study approach," Delft, 2018.

[116] F. F. Alotaibi, "Evaluation and Enhancement of Public Cybersecuirty Awareness," 2019.

[117] A. Solinska-Nowak, P. Magnuszewski, M. Curl, A. French, A. Keating, J. Mochizuki, R. Mechler and M. Kulakowska, "An overview of Serious Games for Disaster Risk Management- Prospects and Limitations for Informing Actions to Arrest Increasing Risk," *International Journal of Disaster Risk Reduction,* pp. 1013-1029, 2018.

[118] S. Turkay and S. Adinolf, "What do players (think they) learn in games?," *Procedia- Social and Behavioral Sciences,* pp. 3345-3349, 2012.

[119] S. Tang and M. Hanneghan, "A Model-Driven Framework to Support Development of Serious Games for Game-based Learning," *IEEE Computer Society,* 2010.

[120] A. All, E. Nunez-Castellar and J.-V. Looy, "Towards a Conceptual Framework for Assessing the Effectiveness of DIgital Game-Based Learning," *Elsevier: Computers and Education,* pp. 29-37, 2015.

[121] D.-M. Lumban-Tobing, E. Utami and H. Al-Fatta, "Analysis of Dominants Game Elements Using the Sillaots Parameters and Octalysis Framework on the Google Play Store," *International Conference Information Technology, Information Systems and Electrical Engineering (ICITISEE),* pp. 484-489, 2019.

[122] M. Eminagaoglu, E. Ucar and S. Eren, "The positive outcomes of information security awareness training in companies: a case study," *Information Security Technical Report 4*, pp. 1-7, 2010.

7 Appendix 1 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Maria Lourdes Bacud

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "Designing Users' Experience Model using Game-Based Learning as capacity building approach in Cybersecurity Awareness for the Public Sector, supervised by Sten Mäses
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.

8 Appendix 2 List of Questions

Interview questions for KII

Cybersecurity Experts

1. Describe the current landscape of the cybersecurity
2. Among the current strategies which are the most efficient and effective? Quick wins and challenges
3. What are the key trends that affect the cybersecurity state and initiatives of your organization?
4. How do you see the possible use of game-based learning as approach to capacity building in cybersecurity awareness initiatives? How can we integrate the

Game-based Learning Experts and Practitioners

1. What are the challenges faced and quick wins of using game based as delivery method or learning?
2. How does game mechanics and learning mechanics optimize learning in your experience?
3. What are the key elements in designing game-based learning? Does game-based learning applicable for every field?
4. How do motivational elements help/ support learning and learning experience of learners/ users?

Focus Group of Discussion

1. Describe your cybersecurity experience (organizational and personal)
2. Describe your experiences on cybersecurity awareness and its direct contribution to their work and personal cyber hygiene
3. What are the hurdles of using users' game experience and perception (advantages and challenges)?
4. How do you think serious games can be incorporated in the cybersecurity awareness test/ training (risk, impediment, goal, needed resources)?