Designing Serious Games for Cyber Ranges: A Socio-technical Approach

Mazaher Kianpour, Stewart James Kowalski, Erjon Zoto, Christopher Frantz and Harald Øverby
Department of Information Security and Communication Technology
Norwegian University of Science and Technology
Gjøvik, Norway
{mazaher.kianpour; stewart.kowalski; erjon.zoto; christopher.frantz; haraldov}@ntnu.no

***Abstract*—Appropriate training is an effective solution to tackle the evolving threat landscape and conflicts in the cyber domain and to fulfill security requirements. Serious games demonstrate pedagogic effectiveness in this field, however, they need to comply with national, organizational, and individual strategies and characteristics. These games provide the players, individually or in groups, with an opportunity to develop their adversarial and system thinking skills to set up effective defenses. To this end, in this paper, we propose a framework for designing serious games that raise security awareness. The proposed framework considers the complex nature of the cyber domain, the knowledge and motivation of participants, and the experiential learning using cyber ranges. The framework is based on existing frameworks, and integrates their advantages to form a comprehensive framework. Future research should refine the framework and design serious games to evaluate its effectiveness in producing desired end results.**

***Index Terms*—cyber range, serious game, cybersecurity education, socio-technical systems, situational leadership**

I. Introduction

The cybersecurity skills shortage is a critical vulnerability for organizations and nations. A survey by McAfee indicates that 82% of respondents report a shortage of cybersecurity skills [1]. This survey looks at four dimensions of cybersecurity workforce development efforts in eight countries: total cybersecurity spending, education programs, employer dynamics, and public policies. The deficit of cybersecurity skills, from technical to organizational, exacerbates the task of managing cybersecurity risks. It shows that conventional training and education could not meet the demand. Our framework quantifies the skill and motivation of cybersecurity workforce and analyzes how cybersecurity stakeholders should build a robust and sustainable set of skills. Learning by experience provides technicians, C-levels and board members with an adequate level of training to bridge the training gaps at all levels of the organizations and governments.

Awareness campaigns used in the majority of cybersecurity education programs typically employ lectures or presentations to state the issues to teach students and employees [2]. Learning methods using this approach are often designed from the perspective of the presenter and focused on delivering information within a minimum amount of time, instead of paying attention to the effective transfer of information [3].

Education theories propose that high quality of information delivery does not necessarily imply optimal learning by the audience. There are other factors such as belief, attitudes, personal knowledge, and perception that can influence awareness substantially. A study by Davinson and Sillence shows that even if training has caused an immediate increase in understanding a topic, it does not essentially reflect the long-term outlook of the audience [4].

Experiential learning is an educational technique in which the learner is directly in touch with the realities being studied. This technique proposes active engagement in developing personal experience scenarios to form the basis of understanding [5]. Serious games are a form of experiential learning that utilize entertainment and simulation to present specific learning objectives and incentivize the player to make decisions, define priorities and solve a given problem [6]. Serious games have been employed in many areas to increase learning, often using simulation as a low-cost alternative for risky or cost-intensive real-life activities. Examples include flight simulators, car and bus simulators, and military strategy games.

Although, there are significant positive impacts of serious games [7], the use of such games do not always lead to optimal learning. Experiments conducted by [3] show that serious games are more effective and involving compared to presentations and multimedia. However, it is challenging to generalize these results to all types of serious games and other learning tools. The reason behind this claim is that the effectiveness of each learning tool depends on the included learning elements and the delivery approach. Experiencing failure, as an important element of learning, in a well-designed serious game provides the participants with the opportunity to reflect on their experiences and develop the mental models of a set of circumstances in which they find themselves. Consequently, they would be able to refine their understanding.

Different personal, social, and environmental factors can affect the cybersecurity risk awareness, decision making process and respective behaviors. In today complex socio-technical systems, these factors interact in complex way and a number of models and approaches have been proposed to describe how these interrelating factors influence human thinking and behavior. Socio-technical systems are referred to as complex, adaptive systems because their emergent properties and asso-

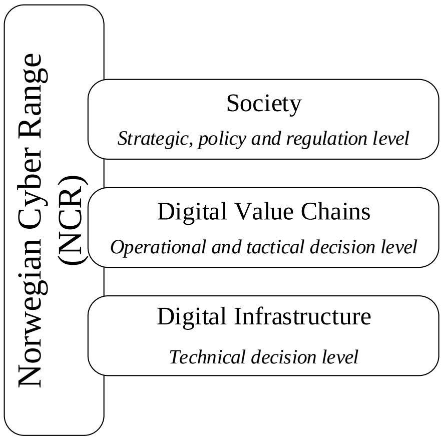
Norwegian Cyber Range (NCR)
Society
Strategic, policy and regulation level
Digital Value Chains
Operational and tactical decision level
Digital Infrastructure
Technical decision level

Fig. 1. Key Levels of the Norwegian Cyber Range

ciated phenomena can have multiple causes and consequences that are highly context dependent, difficult to predict and frequently emerge unexpectedly from the dynamic relationships among system components [32]. Many of these causes and consequences are unforeseen and unintended. We believe that there are significant benefits in employing a socio-technical approach to examine factors that underlie the many different aspects of cybersecurity.

The frameworks proposed in previous studies [7]–[10] are insufficient as a template for cybersecurity because this context presents several new and unique characteristics associated with the digital ecosystem. The area of cybersecurity consists of heterogeneous interacting stakeholders and actors characterized by distinct local cultures, structure, machines, and methods [11]. Stakeholders act upon the basis of their own local states at each given time and interact with other stakeholder at different levels of a complex socio-technical system. These interactions affect future local states and, therefore, create systemic complexity. Geography, location and political boundaries are further factors that are potentially more constraining for regulatory compliance than access limitations.

This lack of integration is a direct result of the absence of an effective framework for implementing cybersecurity training tools. The goal of this study is to develop an initial framework for implementation of serious games in cyber ranges that considers the aforementioned properties. We base our proposed framework on existing frameworks that each has their own benefits and capabilities to meet the requirements of an effective training tool for cybersecurity. Our proposed framework, when fully developed, aims to address a broad range of topics (e.g. policy and decision making, security analysis, etc.) that affect the cybersecurity and resilience of a system. The objective of these games is to explore opportunities for improving cybersecurity posture in the stakeholder's environment, assess the implications of possible solutions, and training the fundamental to advanced concepts of cybersecurity to people characterized with heterogeneous levels of knowledge and motivation.

The rest of this paper is structured as follows: Section II discusses the Norwegian Cyber Range and its goal of providing a training and educational platform to deal with security in complex socio-technical systems. We will review the basic concepts of serious games in Section III. Our proposed framework is discussed in Section IV, outlining the primary components and design guidelines to capture requirements of serious games in cyber ranges using MDA framework. In this section, we also argue the evaluation guidelines of serious games designed using this framework. These guidelines can be also used to evaluate other serious games in the cybersecurity domain. Finally, Section V concludes this paper.

II. The Norwegian Cyber Range

A cyber range is a facility allowing a model of a digital system to run in a simulated environment to perform security tests, training and measurements that are applicable to the real world [33]. Cyber ranges come in various forms distinguished by the size and the complexity of the supported models, the level of detail and realism of the simulated environment, and the scope of possible activities and exercises.

Since each country or organization has a set of unique factors shaping their cybersecurity posture, cyber ranges can be leveraged to develop a stronger cybersecurity workforce and sustain critical skills for cybersecurity professional. Since cyber ranges are controlled, virtual environments where different attack-defense cyber scenarios can be implemented, cybersecurity serious games designed and developed in cyber ranges can improve security professionals' strategies and tactics for defense. Hence, this facilitates skill advancement in organizations by providing solid ideas concerning today's multifaceted cybersecurity challenges.

Norwegian Cyber Range (NCR) is an interdisciplinary arena that will provide better, more realistic education, training, exercises, testing, and research in the context of cybersecurity. Figure 1 shows the three main levels of the NCR approach. The *society level* reflects societal structures and simulates the impact of cyber events with possible chain reactions and the consequences for different levels of society. Such models may be limited to a single business, but may also expand to a region, nation or international entities, depending on the scenario. The *digital value chains* model the extensive networks of producers and consumers of digital services, which often extend across sectors, industries and businesses. Knowledge of the real value chain's composition and extent in which actors are involved and how they are linked together will be of great importance to reflect reality and simulate the consequences of security incidents and business actions. The *digital infrastructure* layer represents the underlying infrastructure, physical or virtual, on which the business operation are running.

This modelling approach increases the precision of understanding the security value chain [37] in the digital ecosystem. The value chains are in fact the level at which the underlying digital infrastructures are linked to the different sectors of society. At this level, NCR enables the users to model security elements in the environment of each stakeholder, test feasibility, usability and security of various technologies, and instantiate complex environments by using efficient automation and orchestration mechanisms. Since NCR has benefited from a deep understanding of cybersecurity challenges, our framework is an adaptation of this approach and is aimed to provide developers of serious games with a meaningful insight into these challenges. Therefore, they can design and develop serious games that keep participants actively engaged and replicate real cybersecurity crisis.

III. Serious Game for Experiential Learning - Definition and Types

Clark Abt's seminal work in [12] and [13] is widely thought to be the originating document behind the term Serious Games [14], as quoted below:

"*Yet individuals can once again become involved, and thought and action can again be integrated, in games created to simulate these social processes. The zest for life felt at those exhilarating moments of history when men participated in effecting great changes on the models of great ideas can be recaptured by simulations of roles in the form of Serious Games*"

Having said that, there are many definitions around the term Serious Games. Abt himself defined them as simulations and games used to improve education, both in and outside of the classroom [12]. The concept was revisited and updated only in the early years of the 21st century, where [15] saw Serious Games are able to connect a serious purpose to the technologies used from the video game industry.

Thus, the Serious Games field has evolved into a real industry through the years, bringing together participants from a wide range of fields, such as Education, Defense, Advertising, Politics, etc., where the domain boundaries are relatively thin [16]. As a result, the actual definition is broader, including any piece of software that merges a non-entertaining purpose with a video game structure [17].

That makes a serious game the kind of game that is designed for a variety of purposes that go beyond pure entertainment [17]. Such purposes have been addressed widely by several researchers in the past decade [18]–[21], detailed further in Table I.

As noticed from Table I, there are some purpose categories which are repetitive, including Activism Games, Advergames or even Business Games and News games. However, more recent work from [17] provides another way of classifying Serious Games based on their purpose. The authors were able to define three purpose-related categories, as follows:

- Message-broadcasting: the game is designed to broadcast a message, which can be educative (Edugames), informative (Newsgames), subjective (Military games) etc.
- Training: the game is designed to improve cognitive performance or motor skills, i.e. Exergames.
- Data exchange: the game is designed as support for exchanging data, usually by collecting information from the players.

Regarding the types of Serious Games, given their divergent primary purposes mentioned above, the field covers a wide range of different games. This makes it hard to devise an appropriate classification method, though during the past years there have been several proposals towards this end.

Initially, the classification methods were more clear-cut, with researchers trying to classify the games landscape based on a set of simple criteria, along with the characterization of the target audience, beyond the already mentioned classification based on the main purpose [21].

On the market side, a range of different categories defined by several authors emerged, such as: Defense/Military, Government, Educational/Training, Health-care, Advertising/Corporate Games etc. [21]–[24]. Table I provides more detailed information on the respective categories. The authors in [21] suggested that a classification system consisting of multiple criteria would be more effective by combining their own market-based and purpose-based classifications into a two-dimensional system. However, in [17] the authors argued that even such a system would not be enough to classify all Serious Games accurately. Hence, they introduced the Gameplay/Purpose/Scope (G/P/S) model. It was seen as a necessary step in such a broad discipline with many overlapping categories and uses. The model would classify each game according to three aspects, listed below:

- Gameplay, intended to provide information about the game structure of the Serious Game: how it is played, i.e. game-based or play-based.
- Purpose, which addresses the eventual purpose(s) apart from entertainment intended by the designer of the game itself.
- Scope, which suggests the actual use(s) related to the game: the kind of market, the audience who uses it.

Figure 2 shows how the classification is conducted within each aspect in more details.

IV. Proposed Framework

The popularity of serious games is growing and various research has been conducted on methodologies for serious

Purpose Categories	Bergeron, 2006	Despont, 2008	Alvarez, 2007	Sawyer and Smith, 2008
	Activism Games	Advert Games	Edugames	Games for Health
	Advergames	Institutional Serious Games	Advergames	Advergames
	Business Games	Business Games	Newsgames	Games for Training
	Exergaming	Learning Games	Activism games	Games for Education
	Health and Medicine Games		Edumarket games	Games for Science and Research
	News Games		Training and Simulation games	Production
	Political Games			Games as Work
Market Categories	Zyda, 2005	Chen and Michael, 2005	Alvarez and Michaud, 2008	Sawyer and Smith, 2008
	Healthcare	Military Games	Defense	Government and NGOs
	Public policy	Government Games	Training and Education	Defense
	Strategic Communication	Educational Games	Advertising	Healthcare
	Defense	Corporate Games	Information and Communication	Marketing and Communication
	Training and Education	Healthcare Games	Health	Education
		Political Games	Culture	Corporate
		Religious Games	Activism	Industry
		Art Games		

TABLE I
PURPOSE AND MARKET CATEGORIES FROM PREVIOUS WORKS

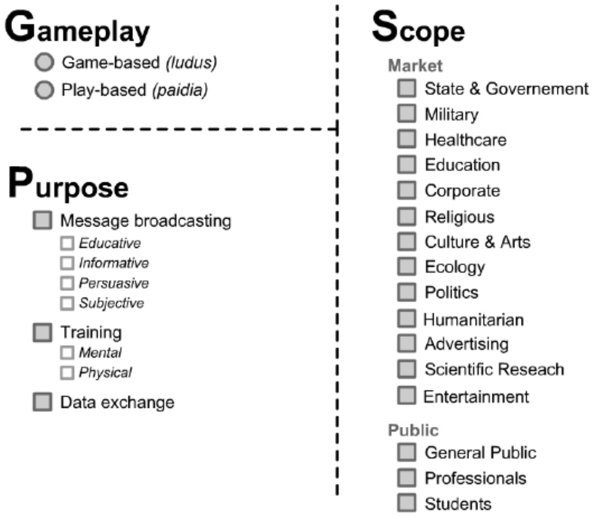

Fig. 2. The G/P/S model defined [17]

games design. However, the researchers have focused on specific aspect of serious games and suggest new approaches in the evaluation of serious games. In this section, we propose a comprehensive framework to design and implement serious games aimed for the cybersecurity context. For our research purposes, we define a framework as a voluntary guidance, based on existing standards and practices for stakeholders to provide them with a common and inclusive depiction of the field of study (cybersecurity) that delivers meaningful insights and a basis for dialog across the ecosystem of stakeholders. In this section we discuss the essential components of our proposed framework, and we describe how they can address the limitation raised in the literature.

A. Socio-technical Framework

The socio-technical framework contains two basic models: a dynamic model of socio-technical changes, called the socio-technical system, and a static one, called the security-by-consensus (SBC) model or stack. As Figure 3 shows, these models can be applied to each stakeholder at different levels of a complex socio-technical system. We define a *secure system* as a system that is resilient against any malicious change in each interrelated sub-component at different levels, and preserves its operational security characteristics, including confidentiality, integrity and availability. The challenge here is that once a level or sub-component of the system is changed, security of other levels and sub-components is affected. Hence, several major changes may be required at the same time to keep the system in an equilibrium state. Otherwise, the system will continue in a state of disequilibrium (insecurity) [30].

Serious games in cyber ranges should present complex environments and the externalities caused by interconnected and inter-dependent stakeholders. Players should be able to explore strategies and policies so that they make more informed decisions related to cybersecurity. However, Meadows argues that a conceptually complex game needs to be relatively simple, in terms of activities, in order to be effective. Therefore, the challenge is designing a game with an appropriate gameplay, engaging model of reality while, at the same time, retaining a sufficiently accurate representation of the fundamental concepts. To achieve this goal, we employed a socio-technical paradigm for the implementation of serious games in cyber ranges to explore a diversity of cybersecurity ecosystems. Values and cultures, for example, are not necessarily prioritized to the same extent in every country. Furthermore, the implementation of optimal cybersecurity strategies requires a meaningful insight on increasingly evolving threat landscape and multidisciplinary challenges such as social, legal, economic and technology in this area.

B. Situational Leadership

Today, most decision makers realize that to succeed in the digital economy, their organizations will need to change. Digital transformation goes beyond just deploying new technical solutions. An effective transformation requires a collaborative effort among involving partners, customers, stakeholders, and their people, in particular. Considering the fact that digital transformation is the most impactful information technology

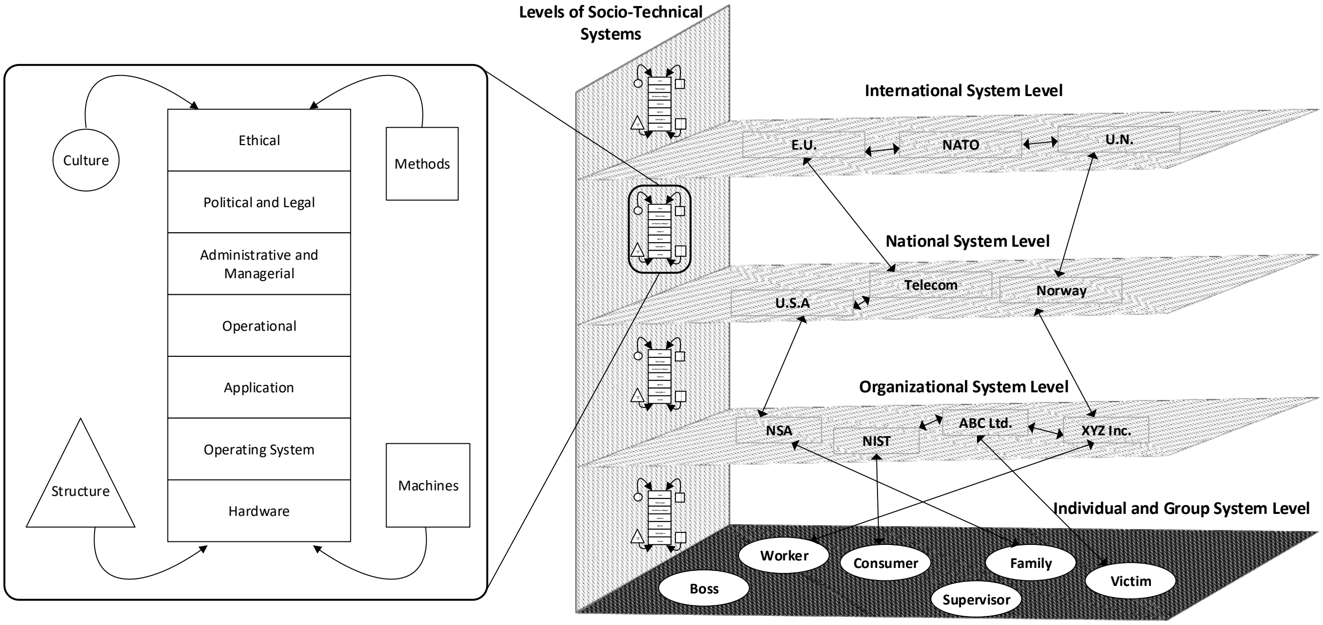

Fig. 3. Interaction among organizations in a socio-technical system is not limited to the organizational level, but also includes different levels of societal actors such as international systems, governments, groups, and individuals levels. Each of these actors has its own particular instruments which can employ different security controls depending on the nature of the system [11]

trend on businesses today, cybersecurity is by far the biggest challenge to these changes [7].

Organizations are dealing with the real and serious business risks related to cybersecurity. Regardless of size, in most organizations, cultivating a culture where all employees understand managing cybersecurity risk is critical. Any organization or nation-wide change, particularly a culture change, succeeds or fails depending on how well the leaders establish the priority and adopt a leadership style characterized by strategic, tactical, and operational support. Creating a culture of cybersecurity risk awareness begins with leadership efforts in these three areas; *cybersecurity training*, *accountability and management of cybersecurity risk*, and *adoption of cybersecurity counter measures* [25].

In our proposed framework, one of the components is the Situational Leadership model. The concepts, procedures, actions, and outcomes derived from this model are based on tested methodologies that are hands-on, real world, and easy to apply. The model provides a framework for leaders (i.e. anyone who is able to influence others, regardless of position) to match their behaviors with the performance needs of the individual or group that they are attempting to influence. It is about adapting the directive and supportive behaviors that leaders use to match the Performance Readiness of others to perform specific tasks or functions [26].

Serious games in the cybersecurity training domain should assess the players knowledge and motivation. Such an assessment may produce four combinations of ability and willingness, with the game mechanics should be designed accordingly. The serious games should determine their style as a function of directive (task-oriented) or supportive (relationship-oriented) behavior. Task-oriented games engages the participants in defining roles, structuring activity and providing the *what*, *where*, *when*, *how* and, if more than one person is involved, *who* is to do what for a particular task. At the same time, relationship-oriented behavior determines the extent to which a participant engages in two-way communication, facilitates interaction and actively listens. Figure 4 show the various combination of task and relationship behavior that define four leadership styles in the Situational Leadership Model. These styles can be employed by games depending upon the assessment of participants' knowledge and motivation (Performance Readiness) in learning cybersecurity skills.

The learning effectiveness depends on the the ability of the game to assess the Performance Readiness of the involved players and provide them with an optimal learning experience. For example, a player with little knowledge and experience would require more direction than a player who has several years of experience. A proper game empowers the player with the required knowledge and motivation to effectively perform the related tasks. Table IV-B shows the corresponding styles of different combinations of participants' knowledge and motivation assessment.

C. Experiential Learning

Schön introduced the concept of reflection in action in his book *"The Reflective Practitioner: How Professionals Think in Action"*. This concept explains how professionals meet

(Knowledge, Motivation)	Leadership Style	Description
(Low, Low)	Telling (S1)	Participants need clear structure and direction.
(Low, High)	Selling (S2)	Participants are inexperienced, but highly motivated, so they need both encouragement and direction. The game clarifies decisions and recognizes the enthusiasm of the participants in an effort to ensure understanding
(High, Low)	Participating (S3)	Participants have a good understanding of what to do, but they need support. The Game and participants attempt to mutually establish alignment.
(High, High)	Delegating (S4)	Participants are motivated, competent and confident. The game allows them to complete tasks.

TABLE II
GAME'S STYLE DEPENDS UPON THE PERFORMANCE READINESS OF THE PARTICIPANTS.

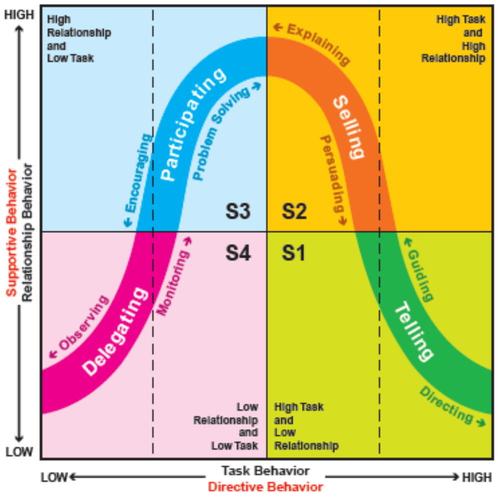

Fig. 4. Leadership Styles [26]

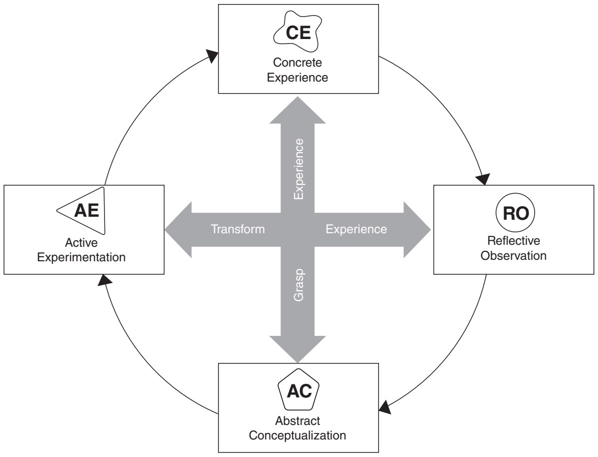

Fig. 5. Kolb's Experiential Learning Cycle [5]

the challenges of their work with a kind of improvisation[1] that is improved through practice [28]. The idea of reflective practice is based upon the assumption that we learn from our experiences and that this contributes to our professional knowledge. David Kolb's theory of experiential learning provides a helpful framework for understanding how reflection helps us make sense of our experiences [5]. Serious games in cyber ranges provide practical activities to people with different knowledge, motivation and responsibilities. Kolb refers to this as the concrete experience that begins the cycle of experiential learning (See Figure 5).

During or after a concrete experience, we often reflect on what we did, what went well and what did not go so well. This is referred to as reflective observation in Kolb's model and highlights the importance of reflecting in and on action in order to learn from experience. This reflection in experience often results in new ideas or conceptualization that shape our learning about practice. Through what Kolb calls abstract conceptualization, we generate new understandings about ourselves and our practices that inform the way we work. We then experiment by trying out these new ideas or conceptualizations as part of the learning process. Through what Kolb calls active experimentation, we test out the implications and validity of our new understandings in the real world and come to integrate new approaches into our practice repertoire. This cyclical process of experiential learning is often repeated in order to see what happens as a result of our adaptations. This process enables the participants to think about new experience, reflect further, draw new conclusions and perhaps decide to adapt to one's practice again.

Not only must reflection be seen to be acceptable, debriefing and subsequent experimentation must be linked to this framework to ensure appropriate mental models are developed by the participants. These allow them to develop the mental models of the situation and refine their understanding of the cybersecurity issues. Lack of mental models is a frequent problem with the cybersecurity arena to help people assess the threats they encounter and maintain their security awareness [29]. Mental models, developed as a result of training and experience in an environment, allow people to predict and explain the behavior of other stakeholders and recognize the relationships among them and the environment. This enables them draw inference, understand the phenomena, decide which actions to take, and experience them.

D. The Framework

Across these frameworks and models, we have found various commonalities in the fundamental requirements, complex systems design, and reflective practice elements that charac-

[1] The activity of making or doing something that you have not planned, using whatever you find (Definition in the Cambridge English Dictionary. dictionary.cambridge.org. Retrieved 2019-02-20.).

terize serious games initiatives in cyber ranges. To facilitate the discussion of these concepts, we use the MDA framework proposed by Hunicke et al. [31]. This framework formalizes theoretical game design using the following concepts:

- **Mechanics** describe the rules and components of the game and the conditions for progress of the player.
- **Dynamics** describe these rules manifest during running the game based on the player's inputs and interactions among the players.
- **Aesthetics** describe the desirable responses by the users interacting with the system.

The MDA framework helps us to conceptualize the relationship between the designer and the player. The designer's perspective links mechanics (functions and features of the game) to dynamics (system-user interaction), and subsequently aesthetics (end-user's emotion and experience). Figure 6 shows our adaptation of the MDA framework. Employing Situational Leadership framework in game mechanics ties to different courses of action that would lead the player to higher levels of cybersecurity awareness. It also enables walk-throughs to unlock a sequence of achievements. Completion of specific learning modules is suggested to allow the player to proceed to next levels.

The socio-technical framework in the game dynamics creates the context of the system to establish a cognitive development for players to recognize affordances the gameplay supports. Such a framework might also involve imposing constraints on the activities based on the current performance readiness of players. Finally, the experiential learning model in game aesthetics allows the players to reflect on challenges, confidence, cognizance, and creativity during their practice. Challenges forces the player to demonstrate decision making and problem solving skills during the interaction with the game. Players reflect their increased awareness and understanding of their environment (cognizance), use of their ideas (creativity), and growing their confidence at their profession.

An effective experience of serious games need to be coherent across these three steps considering the perspective of both the designer (feature-driven) and the player (experience-driven). Business requirements, player characteristics, and behavioral outcomes need to be deliberated during the planning and designing stages of the game. Technologies and tools that would effectively engage players in gamification activities should be considered during the implementation and deployment stages.

E. Evaluation Guidelines

Our proposal is an initial and preliminary framework based on the limitations of specific case studies in our research studies. The applicability of this framework should be measured by its correlation and alignment to real-world requirements, so that any implemented scenario or event in the game will be judged as realistic by the participants. Several key success factors for the design of serious games using this framework are outlined below:

- **Design for effectiveness.** Lack of proper analysis, planning, and cyclical improvement based on the reflections would lead to uncertainties about game's pedagogical effectiveness. Preliminary analysis and the Situational Leadership framework can help ensure that the game meets business objectives and individual outcomes. Reflections can not only be useful in identifying the design flaws, but also they can help in delivering the intended gameplay according the player's responses and dynamics of the environment.
- **Design for coverage.** We believe that cybersecurity is no longer a technical problem and information security discipline would benefit from adopting knowledge, practices, and experience from other fields such as sociology, psychology and economics, rather than seeking purely technical solutions. The serious games in cyber ranges should cover these fields considering the interdependent stakeholders and multidimensional aspects of cybersecurity scenarios.
- **Design for engagement.** The main need for gamification is to keep the participants engaged and motivate them to achieve success through game initiatives and strategies. Designers should ensure engagement using different means such as entertaining activities and providing challenges and rewards. A creative storified context that is linked to the real world scenarios can help motivate participants and provide delightful experiences.
- **Design for reflection in action.** As we highlighted in our discussion on experiential learning and game aesthetics, the participants might show various motivation, emotion and expectations during using the game. Hence, designers should enable the players to reflect in and on action during the game. Toward this objective, different methods like debriefing, survey and post-experiment questions can be used in addition to mechanisms that get the feedback of the player during the game.

Figure 7 shows a diagram that can be employed in concluding analysis and evaluation of key success factors in the serious games implementation. The rating scale of these factors are arbitrary and can be changes based on research plan. This evaluation can help the designers to develop more productive games considering the individuals, groups or businesses objective.

V. Conclusion and Future Work

This paper proposed the a new framework for implementation serious games in cyber ranges. These games are aimed to improve cybersecurity awareness and training. This framework is based on existing frameworks addressing the complexity of cyber domain, unique characteristics of participants, and pedagogic potential of the designed games. It was discussed that how the integration of these frameworks can help to increase the effectiveness, coverage, engagement, and the ability to reflect in practice of games. In order to realize the full potential of this framework and achieve effective guideline for implementation of serious games, we used the MDA

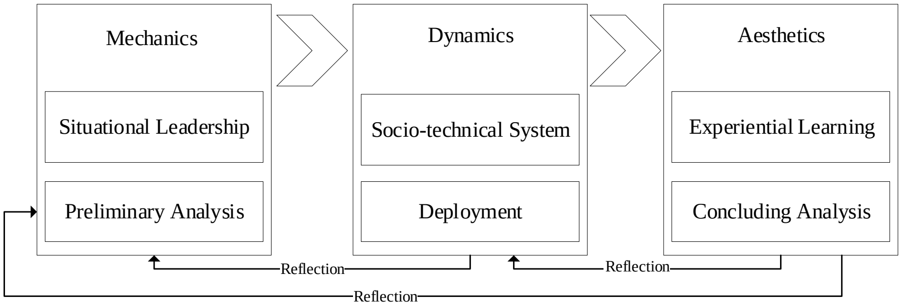

Fig. 6. Proposed Framework

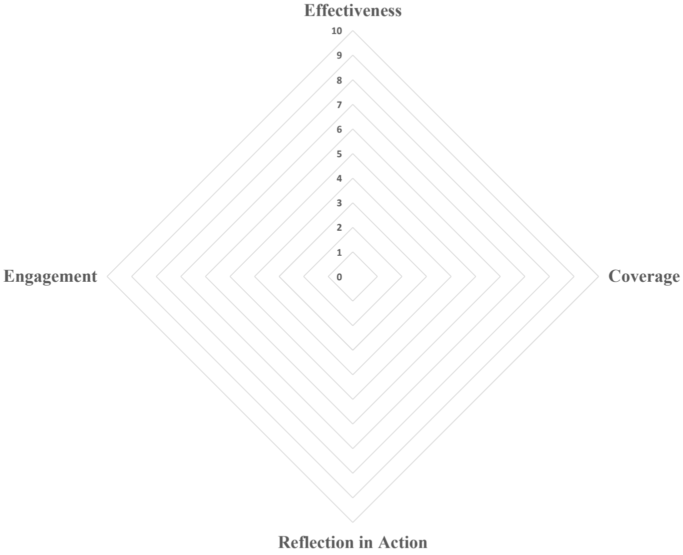

Fig. 7. Game Assessment Criteria by Participants

framework as a practical tool to conceptualize the structure of framework using a systematic approach.

This framework is a preliminary artifact that can be supported or enhanced by other frameworks such as LM-GM [34] and SGDA [35] frameworks. In other words, our research is a call for additional research by researchers in different fields of study to consider features and functions of simulation and gamification to raise cybersecurity awareness at different levels of society. The next step for this research would be implementation of a serious game using this framework and assess the mentioned key success factors in compare with other serious games in cybersecurity domain. The prototype of this game is an extension of agent-based simulation tool which has been developed and demonstrated by the Norwegian Cyber Range.

ACKNOWLEDGEMENT

The authors of this paper would like to sincerely acknowledge Dr. Basel Katt and Ms. Grethe Østby for their constructive comments on this paper.

REFERENCES

[1] Center for Strategic and International Studies. ”Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills.” (2016).

[2] Coventry, Lynne, Pamela Briggs, John Blythe, and Minh Tran. ”Using behavioural insights to improve the public’s use of cyber security best practices.” Gov. UK report (2014).

[3] van Dijk, Tom, Ton Spil, Sanne van der Burg, Ivo Wenzler, and Simon Dalmolen. ”Present or play: the effect of serious gaming on demonstrated behaviour.” International Journal of Game-Based Learning (IJGBL) 5, no. 2 (2015): 55-69.

[4] Davinson, Nicola, and Elizabeth Sillence. ”It won’t happen to me: Promoting secure behaviour among internet users.” Computers in Human Behavior 26, no. 6 (2010): 1739-1747.

[5] Kolb, David A. Experiential learning: Experience as the source of learning and development. FT press, 2014.

[6] Crookall, David. ”Serious games, debriefing, and simulation/gaming as a discipline.” Simulation and gaming 41, no. 6 (2010): 898-920.

[7] Connolly, Thomas M., Elizabeth A. Boyle, Ewan MacArthur, Thomas Hainey, and James M. Boyle. ”A systematic literature review of empirical evidence on computer games and serious games.” Computers and Education 59, no. 2 (2012): 661-686.

[8] Le Compte, Alexis, David Elizondo, and Tim Watson. ”A renewed approach to serious games for cyber security.” In 2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace, pp. 203-216. IEEE, 2015.

[9] Marklund, Bjorn Berg, Per Backlund, and Henrik Engstrom. ”The practicalities of educational games: Challenges of taking games into formal educational settings.” In 2014 6th International Conference on Games and Virtual Worlds for Serious Applications (VS-GAMES), pp. 1-8. IEEE, 2014.

[10] Nagarajan, Ajay, Jan M. Allbeck, Arun Sood, and Terry L. Janssen. ”Exploring game design for cybersecurity training.” In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256-262. IEEE, 2012.

[11] Kowalski, Stewart. ”IT insecurity: A multi-disciplinary inquiry.” (1996): 1081-1081.

[12] Abt, C (1970). Serious Games. USA, Viking Press.

[13] Abt, C.C.: Serious Games. University Press of America (1987)

[14] Wilkinson P. (2016) A Brief History of Serious Games. In: Dörner R., Göbel S., Kickmeier-Rust M., Masuch M., Zweig K. (eds) Entertainment Computing and Serious Games. Lecture Notes in Computer Science, vol 9970. Springer, Cham

[15] Sawyer, B. (2002), Serious Games: Improving Public Policy through Game-based Learning and Simulation. USA, Woodrow Wilson International Center for Scholars.

[16] Corti, K. (2007). Serious Games - Are We Really A Community?. Retrieved February 18, 2019 from https://www.gamasutra.com/view/news/106784/Opinion_Serious_Games__Are_We_Really_A_Community

[17] Classifying Serious Games: The G/P/S Model In Handbook of Research on Improving Learning and Motivation through Educational Games (2011), pp. 118-136, doi:10.4018/978-1-60960-495-0.ch006 by Damien Djaouti, Julian Alvarez, Jean-Pierre Jessel edited by Patrick Felicia

[18] Bergeron, B. (2006). Developing Serious Games. USA, Charles River Media.

[19] Despont, A. (2008), Serious Games et intention sérieuse : typologie. Retrieved February 18, 2019 from http://www.symetrix.fr/20080215serious–games-et-intention-serieuse-typologie/

[20] Alvarez, J., & Rampnoux, O., & Jessel, J-P., & Methel, G. (2007). Serious Game: just a question of posture?. In Artificial and Ambient Intelligence convention (Artificial Societies for Ambient Intelligence) - AISB (ASAMi) 2007 (pp 420-426), UK, University of Newcastle.

[21] Sawyer, B., & Smith, P. (2008, February). Serious Game Taxonomy. Paper presented at the Serious Game Summit 2008, San Francisco, USA.

[22] Zyda, M. (2005). From Visual Simulation to Virtual Reality to Games. Computer, 38(9), 25-32.

[23] Chen, S., & Michael, D. (2005). Serious Games: Games that Educate, Train and Inform. USA, Thomson Course Technology.

[24] Alvarez, J., & Michaud, L. (2008). Serious Games: Advergaming, edugaming, training and more. France, IDATE.

[25] Fortinet, "Security Implications of Digital Transformation Report", 2018.

[26] The Center for Leadership Studies, "Situational Leadership® – Relevant Then, Relevant Now", 2017.

[27] Calderon, A. and Ruiz, M., (2015). "A systematic literature review on serious games evaluation: An application to software project management". Computers & Education, Vol. 87, pp. 396-422.

[28] Schön, Donald A. The reflective practitioner: How professionals think in action. Routledge, 2017.

[29] Blythe, Jim, and L. Jean Camp. "Implementing mental models." In 2012 IEEE symposium on Security and privacy workshops, pp. 86-90. IEEE, 2012.

[30] Al Sabbagh, Bilal, and Stewart Kowalski. "A socio-technical framework for threat modeling a software supply chain." IEEE Security & Privacy 13, no. 4 (2015): 30-39.

[31] Hunicke, Robin, Marc LeBlanc, and Robert Zubek. "MDA: A formal approach to game design and game research." In Proceedings of the AAAI Workshop on Challenges in Game AI, vol. 4, no. 1, p. 1722. 2004.

[32] Hettinger, Lawrence J., Alex Kirlik, Yang Miang Goh, and Peter Buckle. "Modelling and simulation of complex sociotechnical systems: Envisioning and analysing work environments." Ergonomics 58, no. 4 (2015): 600-614.

[33] Winter, H. "System security assessment using a cyber range." (2012): 41-41.

[34] Lim, Theodore, Maira B. Carvalho, Francesco Bellotti, Sylvester Arnab, Sara De Freitas, Sandy Louchart, Neil Suttie, Riccardo Berta, and Alessandro De Gloria. "The lm-gm framework for serious games analysis." Retrieved October 3 (2015): 2015.

[35] Mitgutsch, Konstantin, and Narda Alvarado. "Purposeful by design?: a serious game design assessment framework." In Proceedings of the International Conference on the foundations of digital games, pp. 121-128. ACM, 2012.

[36] Zoto, Erjon, Stewart James Kowalski, Edgar Alonso Lopez Rojas, and Mazaher Kianpour. "Using a socio-technical systems approach to design and support systems thinking in cyber security education." CEUR Workshop Proceedings, 2018.

[37] Alsabbagh, Bilal, and Stewart Kowalski. "A cultural adaption model for global cyber security warning systems." In 5th International Conference on Communications, Networking and Information Technology Dubai, UAE, pp. 16-18. 2011.