# CYBER SECURITY EXERCISE – LITERATURE REVIEW TO PEDAGOGICAL METHODOLOGY

**J. Hautamäki[1], M. Karjalainen[1], T. Hämäläinen[2], P. Häkkinen[2]**

*[1]JAMK University of Applied Sciences (Finland)*
*[2]Jyväskylä University (Finland)*

## Abstract

This paper is a literature review, where we try to find out pedagogical principles has used in different virtual or simulated industry learning environments. The purpose is to use these findings to create in the future a new model for teaching in cyber security exercises. Cyber security exercises are the major service at JYVSECTEC - Jyväskylä Security Technology, cyber security research, training and development center in Finland [1]. JYVSECTEC Cyber security exercises are executed in real life simulation environment, RGCE (Realistic Global Cyber Environment) [1]. It provides the same functionality as the real Internet, but it is isolated from the real Internet and fully controlled by JYVSECTEC, enabling the use of global threats and scenarios [2]. As a result, we found out that there is a limited number of research on cyber security exercise from a pedagogical point of view. We observed that results of studies from other business areas can be applied partly in the development of pedagogical principles of cyber security exercise.

Keywords: Cyber security, exercise, collaborative learning, simulation pedagogy, game based learning.

## 1 INTRODUCTION

Cyber domain is a complex environment where technology, processes and human activities are combined. Effectiveness of incident responses is difficult to predict. This is why the use of a real-like enclosed environment is needed and the learning can be structured in the required areas of competence development.

Teaching methods of cybersecurity have been classroom lectures, home assignments and use of traditional lab environments. By using these traditional methods frequently, the students practice different parts of cybersecurity separately and the big picture including the cause of events occurring in the operating environment is difficult to teach. In recent years the use of cyber ranges as an educational environment has seen significant growth [3], [4], [5]. There are different types of exercise methodologies based on international standard ISO-22398 [6] and the following types of methods have followed out: capture the flag, discussion based game, red team blue team, seminar, simulation, tabletop and workshop methods. Although the use of cyber security exercises as a method of knowledge development for individuals and organizations has increased, the pedagogical theory of exercises has not been studied.

Cyber security exercises provide opportunities for organizations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. The exercises can help train organizations to improve their ability to mitigate impacts of cyber threats and attacks to business [1].

Cyber exercise is a special case of learning. Gurnami et al. divide cyber security exercise into two different categories: discussion-based exercise and operation-based exercise [7]. The article explains why cyber security exercise is a good way to train an organization. The paper also contains statistics on quantitative increase in training.

In another paper, Ferette [5] introduces global statistic of cyber security exercises. The paper is a study where he has gathered and analyzed a primary dataset as the first step towards an EU-wide dataset on cybersecurity exercises. The paper also introduces different types of training methods.

Furtuna et al. present in their paper that cybersecurity exercises are a very effective way of learning and practicing different aspects of cyber security [8]. Designing and implementing a cyber security exercise requires detailed planning and detailed instructions for performing a complex task. Because of this, it

also has many forms and approaches. The paper presents a step-by-step implementation of a cyber security exercise and design considerations for different phases.

Vykopal et al. introduce in their paper experiences of using cyber security exercise in education [9]. The paper identifies a general life cycle of a cyber defence exercise. The exercise consists of five phases: preparation, dry run, execution, evaluation, and repetition. The exercise has two special challenges, design of testing and sufficient individual and team feedback from the exercise execution.

In a cyber security exercise generally, an individual acts as part of a team in a predetermined role. Working as a part of a team enables the integration of training into the organization's genuine functions, thus enabling the development of organizational functions. In accordance with the goals of the exercise, a scenario is made for the exercise, which enables the execution of the exercise objectives.

The teams in the exercise are the Blue Team, the White Team, the Red Team, the Green Team, and possibly research teams, often called the Purple Team. The Blue Team defends their fictional organization environment, The Red Team is a threat actor, The Green Team is in charge of the construction and maintenance of exercise infrastructure and the White Team is the leading team. The Purple Team observes and researches actions.

Based on earlier research, this paper assesses pedagogical principles implemented in cyber security exercises. The study perspective is based on collaboration and simulation of real life events in exercises. Games and simulation are powerful methods when the focus in an education event is on student performance, engagement, and learning motivation [10]. Simulation is one of the seven game pedagogy genres (action, adventures, fighting, role-playing, simulations, sports and strategy games) with game modelled natural or man-made systems or phenomena. Students act as players with pre-specified goals that they try to achieve [11]. In simulation, a scenario-based environment will be created where students try to solve real life problems and increase their knowledge by applying their previous experiences [12].

JAMK University of Applied Sciences hosts a cyber security research, development, and training center JYVSECTEC (Jyväskylä Security Technology). It provides a real value for customers and accelerates the technological development and preparedness against threats. It offers cyber security related services, e.g. cyber security exercises, personnel training, software testing, and management consulting as well as accreditation and certification functionalities. [1]

Cyber security exercises are the major service at JYVSECTEC. Cyber security exercises are executed in real life simulation environment, RGCE (Realistic Global Cyber Environment).

The organization participating in exercises can engage in cyber exercise with different functionalities or persons acting in different roles such as technical persons, process management or business management. The goal is to train individuals and by the increased knowledge of individuals improve the organization’s ability to handle and tolerate cyber threats. There are often two or more organizations participating in the exercise, which enables the network of partners and subcontractors to develop their resilience. JYVSECTEC mindset is to provide a variety of scenarios simulating threat actors that are threat-driven with their tactics, techniques and procedures (TTPs) [1].

# 2 LITERATURE REVIEW

Keywords in the literature review have been categorized to the three sub categories: Game based learning, Simulation and Collaborative learning. In all these subcategories, we used several keywords. These keywords in database search have been selected because these principles have been fundamental in planning of JYVSECTEC environment. Articles have been evaluated against cyber security exercise concept and 32 articles were chosen to the deeper review. Databases where articles were found were ABI/Inform, Ebsco, DOAJ, Elsevier ScienceDirect, IEEE Explore and ISO standard catalogue.

## 2.1 Game Based Learning

Game based learning (GBL) as a term reflects a teaching approach where students perform game-related tasks in a learning environment designed by teachers. Teachers and students collaborate in order to add depth and perspective to the experience of playing the game. Teachers and students collaborate on a gaming event that provides depth and a new perspective on learning.

Learning processes are in a major role in GBL. Bariran et al. [13] investigated in their paper the effect of mutual interactions on students’ learning process. Research tools in this paper are supply chain total cost and ordering fluctuations as critical measurement criteria. The research has been conducted with

a beer game software, which is an effective outcome-based evaluation tool for individual measurement of learner's progress.

Emin-Martinez and Muriel [14] continue in their paper with the same perspective. The paper introduces a model for the process of teachers' adoption of Game Based Learning (GBL). The results have been evaluated based on the authors' own model which has been concluded from modified Roger's "Perceived Attributes of Innovations " model and adopted to (GBL) context. Serious games is one of the forms of manifestation of (GBL) [15].

The use of games and simulations have been researched as a tool for higher education for preparation of future professionals in education [10]. The research result indicates that use of games and simulations in a suitable amount has a positive impact on achieving learning goals.

## 2.2 Simulation

Combination of game pedagogy and simulation is one of the interesting solutions [13]. The beer game is a role play simulation that introduces the participants to typical coordination problems of supply chain. In more general terms, this supply chain represents any non-coordinated system where problems arise due to lack of systemic thinking.

Otherwise, it has also been claimed that simulation is not pedagogy [16]. Simulation is an immersive teaching / learning platform, which is a representation of a functioning system or process. The paper describes a lack of research about pedagogies appropriate in the area of using simulation as a learning platform.

Simulation means an artificial representation of real world processes aimed at achieving educational goals through experiential learning [17].

The debriefing phase is one of the important phases in simulation learning [18]. In this paper, researchers used eighteen video-recorded debriefing sessions and analysed them collaboratively. The study result indicated that learning outcomes emerged whether a specific structure of debriefing was used or not.

Kalalahti has studied the pedagogical use of simulation in the training of security professionals under the Ministry of the Interior [19]. The research collected information using case study method from Police University College, Emergency Services College, Crisis Management Centre Finland and Border and Coast Guard Academy. The aim was to study how the simulation fits to the training programs, and collect the existing best practices. A case study based research findings were that from the learning point the simulation scenarios were not so important than the debriefing part after the simulation exercise. Important finding were also that the orientation of students before the simulation exercise was essential for achieving good learning outcomes.

In the cyber security exercise, interaction is emphasized during the session. Ngyuen et al. in their paper introduce a meta-model, which promotes identifying collaboration in three dimensions of simulation: simulator, role and user [20]. The purpose of meta-model is to help interactions during the simulation process.

Dohaney introduces in her paper an interactive role-play simulation where the focus is to forecast and mitigate a volcanic crisis in [21]. It was found that students liked this kind of role-play and their skills were improved. Students appreciated especially the authenticity and challenging nature of the role-play.

Borštnar introduces in her paper the results from experiences to use two simulation models in teaching [22]. In Case 1, learning is based on a simulation model where decision tasks are precisely defined. The study comes to a conclusion that simulation promotes better understanding of the studied problem, solutions are found faster and confidence with course studies is strengthened among participants. In Case 2, the simulation environment is based on social media. In both cases, the participants shared the same opinion that a clear description of the problem made it easier to find a solution.

New sociomaterial theories have emerged on questions of using simulation in higher education [23]. The paper discusses simulating theory and practices in the healthcare industry. The main questions to ask are "What is being simulated?", "Realism versus effectiveness?", "How realistic is this simulation?", "How realistic should it be to enable students to learn to do particular things?" turn out not to be very important at all. This paper responds to repeated calls to enrich and extend the theoretical basis for research and pedagogic practice.

## 2.3 Collaborative learning

What is Collaborative learning? Dillenbourg describes the term as a situation where several people learn or attempt to learn something together [24]. It covers all kind of learning situations, where individual persons use other group members as cognitive resource.

Lelardeux et al. present in their paper a collaborative training method in risk management [25]. The paper introduces how to design educational scenario to improve teamwork, communication, leadership, decision-making and situation awareness. It is important to create a training environment which improves its participants' non-technical skills.

Collaborative learning can be facilitated in many ways. Computer-supported collaborative learning (CSCL) offers many advantages e.g. for communication, monitoring and evaluation. In a computer-supported collaborative learning, the most important issue is to pay attention to how students co-regulate to learn collaboratively [26]. In computer-supported collaborative learning, co-regulation gains the important role where the most important co-regulatory practices are proactive measures and pre-planning [27].

The Computer-supported collaborative learning is an effective tool in training modern engineers. Collaborative learning method offers structured learning strategy for small groups in common studies with collective target [28].

## 3 RESULTS

The purpose of this study was to explore what kind of learning methods have been used in different industry areas when using various types of exercise or training methods.

The literature review was conducted by using keywords, which have been categorized to three categories and subcategories. The categories are Game Based Learning (GBL) articles, Simulation articles and Collaborative Learning (CL) articles. The total sum of selected articles is 32. The articles have been selected from databases based on how the results of the studies can be utilized in cyber security exercises. The articles have been are divided into six different groups based on the study subject: Healthcare, Engineering, Law studies, No area, Other and Cyber security. "No area" indicates a subject which has not been identified and "Other" means a scattered set of study subjects.

The results have been described in table 1.

*Table 1. Overview of reviewed articles .*

| | GBL | Sim | CL | Sum |
|---|---|---|---|---|
| Healtcare | | 4 | | 4 |
| Engineering | 1 | 6 | 1 | 8 |
| Law studies | | 1 | | 1 |
| No area | 2 | 1 | 5 | 8 |
| Other | 1 | 7 | | 8 |
| Cyber security | | 2 | 1 | 3 |
| **Sum** | **4** | **21** | **7** | **32** |

GBL = Game Based Learning

Sim = Simulaltion

CL = Collaborative learning

The most significant part of articles was gathered from engineering education (8). Most of these articles related to simulation (6). Two of the articles referred to game based learning and collaborative learning studies. "No education area" and "other education" comprised the same number (8) of articles. Most of "No area" articles (5) affiliated to collaborative learning studies. In "Other" class most of the articles affiliated to simulation studies (7). In both categories only one or two articles related to game based learning (2 and 1), and collaborative simulation (2). Only three articles were gathered from the field of

cyber security. Two of them related to simulation study and one to collaborative learning. In total, most of the articles related to simulation study (21). The second biggest study subject was collaborative learning (7). Game based learning (4) gathered the smallest number from the articles.

## 4 CONCLUSIONS

As a conclusion of this study, it can be stated that there are few articles related to the study of cyber security exercise. Similarly, there are hardly any studies of pedagogical practices in cyber security domain.

Based in the articles reviewed in this study, it can be observed that results of studies from other business areas can be applied partly in the development of pedagogical principles of cyber security exercise.

Due to the complexity of the cyber security environment, the pedagogy of cyber security exercise requires further research, and from the perspective of learning, reaching an understanding of the cause and effect relationship presents specific challenges. In order to be able to study pedagogical principles and practices, the environment used in the study must be realistic and complex enough. To enable education and research in this field, several massive simulation environments are being built at the global level.

## REFERENCES


[1] "https://jyvsectec.fi/," 2013. [Online]. [Accessed 23 11 2018].

[2] S. Puuska, T. Kokkonen, J. Alatalo, and E. Heilimo, “Anomaly-based network intrusion detection using wavelets and adversarial autoencoders,” 2018, accepted in the International Conference on Information Technology and Communications Security, SECITC, 8-9 November 2018. Will be published in Lecture Notes in Computer Science by Springer

[3] A. Davis T. Leek M. Zhivich K. Gwinnup W. Leonard "The fun and future of ctf" in 2014 USENIX Summit on Gaming Games and Gamification in Security Education (3GSE 14) San Diego CA:USENIX Association. 2014.

[4] Cyber defence exercises. [online] Available: http://ccdcoe.org/event/cyber-defence-exercises.html. [Accessed 14.1.2019].

[5] L. Ferette, “The 2015 report on national and international cyber security exercises “,European Union Agency for Network and Information Security, 2015

[6] Societal security -- Guidelines for exercises. [online] Available: “https://www.iso.org/standard/50294.html. [Accessed 14.1.2019].

[7] R. Gurnani, K. Pandey, S. K. Rai, “A Scalable Model for Implementing Cyber Security Exercises”, International Conference on Computing for Sustainable Global Development (INDIACom). 2014.

[8] A. Furtună, V. Patriciu and I. Bica, "A structured approach for implementing cyber security exercises," 2010 8th International Conference on Communications, Bucharest, pp. 415-418. 2010.

[9] J. Vykopal, M. Vizvary, R. Oslejsek, P. Celeda and D. Tovarnak, "Lessons learned from complex hands-on defence exercises in a cyber range," 2017 IEEE Frontiers in Education Conference (FIE), Indianapolis, IN, pp. 1-8. 2017.

[10] D. Vlachopoulos, A, Makri, "The effect of games and simulations on higher education: A systematic literature review.," in International Journal of Educational Technology in Higher Education 14, no. 1 (2017): 1-33, 2017.

[11] B. Gros, "Digital games in education," in Journal of Research on Technology in Education, 40:1, 23-38, 2014.

[12] M. A. Andreu-Andre's and M. Garcia-Casas, "Perceptions of gaming as experiential learning by engineering students," in International Journal of Engineering Education, 27(4), 795–804., 2011.

[13] S.E.S. Bariran, K.S.M. Sahari, B. Yunus, “A Novel Interactive OBE Approach in SCM Pedagogy Using Beer Game Simulation Theory”, International Journal of Asian Social Science, 2013, 3(9):2034-2040. 2013.

[14] V. Emin-Martinez, N. Muriel, “Supporting Teachers in the Process of Adoption of Game Based Learning Pedagogy”, ECGBL 2013 - European Conference on Games Based Learning, 2013.

[15] M. Cheng, "The Use of Serious Games in Science Education: A Review of Selected Empirical Research From 2002 to 2013." Journal of Computers in Education 2.3: 353-375. 2015.

[16] G. D. Erlam, L. Smythe, V. Wright-St Clair, “Simulation Is Not a Pedagogy”, Open Journal of Nursing, 7, 779-787, 2017.

[17] J. Family, “Simulation-based medical teaching and learning”, Community Med. 17(1): 35–40, 2010.

[18] S. Nyström, "Debriefing Practices in Interprofessional Simulation With Students: A Sociomaterial Perspective." Bmc Medical Education 16.148: 1-8. 2016

[19] J. Kalalahti, Poliisiammattikorkeakoulun raportteja, Poliisiammattikorkeakoulu, 2016.

[20] T. K. Nguyen, N. Marilleau, T. V. Ho, A. El Fallah Seghrouchni, “A Meta-Model for Specifying Collaborative Simulation”. 2010.

[21] J. Dohaney, "Training in Crisis Communication and Volcanic Eruption Forecasting: Design and Evaluation of an Authentic Role-play Simulation." Journal of Applied Volcanology 4.1 (2015): 1-26.

[22] M. Kljajić Borštnar. "Comparative Analysis of Collaborative and Simulation Based Learning in the Management Environment." Organizacija 45.5 (2012): 236-245.

[23] N. Hopwood, D. Rooney, D. Boud, M. Kelly, “Simulation in Higher Education: A Sociomaterial View”. Educational Philosophy and Theory, Pages 165-178, 2014.

[24] P. Dillenbourg, “Collaborative Learning: Cognitive and Computational Approaches. Advances in Learning and Instruction Series”, Elsevier Science, 1999.

[25] C. Pons Lelardeux, M. Galaup, D. Panzoli, P. Lagarrigue, "A Method to Design a Multi-Player Educational Scenario to Make Interdisciplinary Teams Experiment Risk Management Situation in a Digital Collaborative Learning Game: A Case of Study in Healthcare." International Journal of Engineering Pedagogy (iJEP) 8.2: 88-100. 2018

[26] C. Chan, "Co-regulation of Learning in Computer-supported Collaborative Learning Environments: A Discussion." Metacognition and Learning 7.1: 63-73. 2012.

[27] L. Zheng, "Exploring the Behavioral Patterns of Co-regulation in Mobile Computer-supported Collaborative Learning." Smart Learning Environments 3.1: 1-20. 2016

[28] Sumtsova, "Collaborative Learning at Engineering Universities: Benefits and Challenges." International Journal of Emerging Technologies in Learning (iJET) 13.1: 160-177. 2018