JYU DISSERTATIONS 402

Mika Karjalainen

Pedagogical Basis of Live Cybersecurity Exercises

UNIVERSITY OF JYVÄSKYLÄ
FACULTY OF INFORMATION
TECHNOLOGY

JYU DISSERTATIONS 402

Mika Karjalainen

Pedagogical Basis of Live Cybersecurity Exercises

Esitetään Jyväskylän yliopiston informaatioteknologian tiedekunnan suostumuksella
julkisesti tarkastettavaksi kesäkuun 14. päivänä 2021 kello 12.

Academic dissertation to be publicly discussed, by permission of
the Faculty of Information Technology of the University of Jyväskylä,
on June 14, 2021 at 12 o'clock.

JYVÄSKYLÄN YLIOPISTO
UNIVERSITY OF JYVÄSKYLÄ

JYVÄSKYLÄ 2021

Editors
Marja-Leena Rantalainen
Faculty of Information Technology, University of Jyväskylä
Ville Korkiakangas
Open Science Centre, University of Jyväskylä

ISBN 978-951-39-8738-1 (PDF)
URN:ISBN:978-951-39-8738-1
ISSN 2489-9003

Permanent link to this publication: http://urn.fi/URN:ISBN:978-951-39-8738-1

ABSTRACT

Karjalainen, Mika
Pedagogical Basis of Live Cybersecurity Exercises
Jyväskylä: University of Jyväskylä, 2021, 62 p. (plus included articles)
(JYU Dissertations
ISSN 2489-9003; 402)
ISBN 978-951-39-8738-1 (PDF)

The digitalisation of societies, working life, and education is changing their forms and practices. As a component of digitalisation and new ways of operating in a digital domain, change has also brought with it new risks for the digital operating environment. ICT infrastructure constitutes a critical new development, and cybersecurity competency needs for managing digital domains are growing and evolving. To provide the knowledge and skills needed for working life, education and training environments must also evolve in response to change. As part of cybersecurity education, cybersecurity exercises have an established position in competency development.

This study examined the pedagogical principles of cybersecurity training and identified the pedagogical requirements for a comprehensive cyber arena-style education platform. The learning of individuals was measured through both on-site and online cybersecurity exercises. Methodologies for evaluating cybersecurity exercises were studied as part of the exercise lifecycle. The study also examined the requirements for continuous learning from both curriculum design and cybersecurity in-service training perspectives.

Keywords: cybersecurity, cybersecurity exercise, cybersecurity education, in-service training, cyber range, cyber arena, pedagogy

TIIVISTELMÄ (ABSTRACT IN FINNISH)

Karjalainen, Mika
Kyberturvallisuusharjoitusten pedagogiikka
Jyväskylä: Jyväskylän yliopisto, 2021, 62 s. (+ sisältyvät artikkelit)
(JYU Dissertations
ISSN 2489-9003; 402)
ISBN 978-951-39-8738-1 (PDF)

Yhteiskuntien, työelämän ja koulutuksen digitalisoituminen muuttaa kaikkien edellä mainittujen muotoa ja toimintatapoja. Osana digitalisoitumista ja sen mukanaan tuomia uusia toimintatapoja on muutos tuonut mukanaan myös uusia digitaaliseen toimintaympäristöön liittyviä riskejä. ICT-infrastruktuuri muodostaa kaikkinensa uuden kriittisen infrastruktuurin, jonka hallitsemiseksi kyberturvallisuuden osaamistarpeet kasvavat ja kehittyvät koko ajan. Jotta koulutuksessa kyetään antamaan sellaiset tiedot ja taidot, joita työelämässä tarvitaan, tulee myös koulutuksen ja koulutusympäristöjen kehittyä muutoksen mukana. Osana kyberturvallisuuden koulutusta on kyberturvallisuuden harjoitustoiminta vakiinnuttanut asemansa osaamisen kehittämisessä.

Tässä tutkimuksessa tutkittiin kyberturvallisuusharjoittelun pedagogisia periaatteita ja niiden mukaisesti muodostettiin Cyber Arena -tyylisen kyberturvallisuuden harjoitusalustan pedagogiset vaatimukset. Yksilön oppimista kyberturvallisuusharjoituksessa mitattiin On-Site- sekä On-Line-metodilla järjestetyssä harjoituksessa. Kyberharjoitusten arvioinnin metodologiaa tutkittiin osana harjoituksen elinkaaren toiminteita. Tutkimuksessa tutkittiin myös jatkuvan oppimisen vaatimuksia niin opetussuunnitelmien suunnittelutyön kuin täydennyskoulutuksena annettavien kyberturvallisuusharjoitusten näkökulmasta.

Avainsanat: kyberturvallisuus, kyberturvallisuusharjoitus, kyberturvallisuuskoulutus, täydennyskoulutus, kyberturvallisuusharjoitusalusta, pedagogiikka

Author

Mika Karjalainen
Faculty of Information Technology
University of Jyväskylä
Finland

Supervisors

Professor of Practice Martti Lehto
Faculty of Information Technology
University of Jyväskylä
Finland

Professor Tommi Kärkkäinen
Faculty of Information Technology
University of Jyväskylä
Finland

Principal Lecturer Tero Kokkonen
School of Technology
Jyväskylä University of Applied Sciences
Finland

Reviewers

Professor Matthew Warren
College of Business
RMIT University
Australia

Professor Kirsi Helkala
Norwegian Defense University College/
Norwegian Defense Cyber Academy
Norway

Opponent

Associate Professor Mikko-Jussi Laakso
Department of Computing
University of Turku
Finland

ACKNOWLEDGEMENTS

I would like to express my sincerest gratitude to the Jyväskylä University of Applied Sciences, the Institute of Information School Technology lecturers, and cyber security specialists. It has been a wonderful experience to work with a team of top cybersecurity professionals. Their knowledge, insights, guidance, and opinions have made it possible for me to conduct this research.

I would also like to thank the Faculty of Information Technology, University of Jyväskylä, for the opportunity to write this dissertation. In particular, I express my gratitude to my supervisors Professor of Practice Martti Lehto, Professor Tommi Kärkkäinen, and PhD Adjunct Professor Tero Kokkonen for their guidance on this dissertation.

I also wish to thank Jari Hautamäki, Samir Puuska, Niko Taari, Karo Saharinen, Mika Rantonen, and Anna-Liisa Ojala for working as co-authors on the included papers. I thank Tuula Kotikoski and Tim Whale for the proofreading, and Heli Sutinen, Heikki Salo, and Marko Vatanen for assistance with the figures.

I also send sincere thanks to my parents and family for their continuing support and guidance on finding my path.

Jyväskylä 20.5.2021
Mika Karjalainen

LIST OF INCLUDED ARTICLES

I Hautamäki, J., Karjalainen, M., Hämäläinen, T., & Häkkinen, P. (2019). Cyber security exercise: Literature review of pedagogical methodology. In L. G. Chova, A. L. Martínez, & I. C. Torres (Eds.), *INTED 2019: 13th Annual International Technology, Education and Development Conference, Proceedings* (pp. 3893–3898). IATED.

II Karjalainen, M., Kokkonen, T. & Puuska, S. (2019). Pedagogical aspects of cyber security exercises. In *2019 IEEE European Symposium on Security and Privacy Workshops (Euro S&PW)* (pp. 103-108). IEEE.

III Karjalainen, M, Puuska, S, & Kokkonen, T. (2020). Measuring learning in a cyber security exercise. In *ICETC'20: 2020 12th International Conference on Education Technology and Computers* (pp. 205-209). ACM, New York.

IV Karjalainen, M. & Kokkonen, T. (2020). Comprehensive cyber arena: The next generation cyber range. In *2020 IEEE European Symposium on Security and Privacy Workshops (Euro S&PW)* (pp. 11-16). IEEE.

V Karjalainen, M. & Kokkonen, T. (2020). Review of pedagogical principles of cyber security exercises. *Advances in Science, Technology and Engineering Systems Journal,* 5(5), 592-600.

VI Karjalainen, M., Kokkonen, T., & Taari, N. (2021). Key elements of on-line cyber security exercise and survey of learning during the on-line cyber security exercise. In *Cyber Security: Critical Infrastructure Protection*. Springer, to appear.

VII Saharinen, K., Karjalainen, M., & Kokkonen, T. (2019). A design model for a degree programme in cyber security. In *ICETC 2019: Proceedings of the 2019 11th International Conference on Education Technology and Computers* (pp. 3–7). ACM, New York.

VIII Rantonen, M. & Karjalainen, M. (2020). Conversion of emerging ICT-technology info curriculum courses. *Journal of Strategic Innovation and Sustainability, 15*(3), 70–77.

IX Karjalainen, M. & Ojala, A-L. (2021). Authentic learning environment for in-service trainings of cyber security: A qualitative study. *International Journal of Continuing Engineering Education and Life-Long Learning.* Accepted/In print.

FIGURES

TABLES

CONTENTS

1 INTRODUCTION

This study examined the use of cybersecurity exercises as a teaching method and a learning platform. The research mapped the learning of individuals engaging in cybersecurity exercises and determined the requirements for the learning environment as a learning facilitator.

1.1 Research motivation

Cybersecurity training environments (cyber ranges) have largely been developed from the perspective of technical functionalities (Ferguson et al., 2014; Nevavuori & Kokkonen 2019; Newhouse et al. 2017). Thus, the focus has been on the technical functionalities to be included in the environment, rather than the competency objectives or pedagogical models to be used for competency development (Chen et al., 2018; Deckard 2018; He et al., 2019; Yamin et al., 2019). The literature review conducted by Švábenský (2020) indicated that research on cybersecurity education is fragmented and therefore unlikely to support readers interested in cybersecurity education.

The aim of this dissertation was to study the pedagogical theory relating to cybersecurity exercises, to create a new understanding of learning during cybersecurity training, and to evaluate methods for measuring the levels of competence facilitated by cybersecurity exercises. Learning was evaluated in a realistic global cyber environment (RGCE) developed and operated by Jyväskylä University of Applied Sciences and used as a cybersecurity teaching environment. To measure the competency development of students participating in cybersecurity exercises in the RGCE, the research developed a set of indicators for substantive areas and tested their application. Research data were thus obtained regarding the suitability of cybersecurity exercises as competency developers. As part of the research, the functional requirements for the cybersecurity training environment were studied from the perspective of pedagogical requirements. The aim of the study was to develop a set of indicators for measuring students' competency development through such exercises and to identify the requirements for the functionality of the training platform from a pedagogical perspective.

1.2 Research questions

The aim of this study was to develop an understanding of how competency development in cybersecurity practice can be measured and to verify how cybersecurity exercises work as a pedagogical method for competency development. We used metrics developed in the study to measure learning. The study also defined the pedagogical requirements for the cybersecurity training platform to enable exercises to support the competencies that students would need in their post-study working lives.

The research verified how the cybersecurity exercise developed students' competencies and what functionalities should be included in the learning environment to match the learning with the competencies required by students for employment. The objectives of the study were pursued through the following research questions:

1. How does a cybersecurity exercise serve as a tool for developing the competencies of individuals?
   a. How can competency development be measured effectively?
   b. How do students develop their knowledge during such exercises?
2. What underlying pedagogical principles should a cybersecurity training platform be based on?
3. How can cybersecurity exercises support lifelong learning:
   a. for curriculum development in education leading to a degree?
   b. for in-service education?

1.3 Structure of the dissertation

The research questions were answered in nine publications included in the study, and this dissertation is structured as follows. The introduction to the research, the research motivation, and the research questions are presented in Section 1. The background and rationale of the research are defined in Section 2, which also introduces the development of cybersecurity phenomena and relevant key terminology. The section presents the development of engineering laboratory education and its differences from cybersecurity exercises, then discusses the different types of cybersecurity exercises. Section 3 outlines the research methodology used in the study and its applications in the different phases of the study, together with the collected research data and their use.

Section 4 presents the contributions of the mentioned papers to the overall study, as well as the work performed by the author for each study. The section introduces the pedagogical framework for cybersecurity training and discusses key theories relating to cybersecurity exercises. The theory is linked to the lifecycle of a cybersecurity exercise and the practical application of pedagogical targets during all stages of the exercise. The pedagogical requirements for the training platform, and the cyber arena cybersecurity training platform model based on them, are placed in a pedagogical context. Cyber security training is discussed in terms of both education leading to a university degree and in-service training for professionals already in employment. The section introduces curriculum work-related models and specific features and requirements relating to continuing education, since cyber security exercises can be organised as either on-site exercises or online learning events. A questionnaire was developed to measure the levels of students' competencies before and after the exercise. Learning in the exercise was measured for both the on-site and online exercises. Section presents the results of the students' competency level measurement. Section also describes the collaborative environment used for the online exercise. The content requirements and functionalities of in-service training, as reflected in cybersecurity exercises organised as in-service training. Finally, Section 5 presents the conclusions of the study, its limitations, and opportunities for future research.

2 BACKGROUND OF THE RESEARCH

This chapter describes the research framework and its evolution, combining discussion of cyber security domain changes with explanation of the researcher's motivation and research focus. The section also defines the key terms for, and the evolution of, cybersecurity education and training as used in the study.

2.1 Cybersecurity

Digital operating environments are at the very core of modern society. The global digital operating environment, consisting of information systems, servers, terminals, wired and wireless data networks, and people using the former and/or other physical infrastructure, has enabled new enterprises, ways of communicating, and ways of working to evolve (Pöyhönen & Lehto, 2020). Along with opportunities, this change has resulted in prevalent new threats. The global digital operating environment and its connection to the physical world is a complex entity, with functionalities and impacts that are difficult to comprehend and foresee (Sinha, 2014; Törngren & Grogan, 2018). Cybersecurity for managing these digital threats is technologically evolving, multidisciplinary, and continuously expanding (Moser & Cohen, 2013).

The phenomenon of cyber security emerged in the mid-1990s (Warner, 2012), and there are several definitions of cybersecurity. For example, Lubick's definition divides the cybersecurity operating environment into five different layers: a physical layer, a syntactic layer, a semantic layer, a service layer, and a cognitive layer (Libicki, 2007). The physical layer consists of the technical infrastructure. In the cyber domain, special attention should be paid to the technical development of the operating environment, since the technical environment constitutes an ever-changing vulnerability vector. The syntactic layer determines how information system architecture is managed, connected, and controlled. It can be seen as the software layer that sends information and instructions to the physical layer. The semantic layer consists of the interactions of, and information generated by, humans and different technologies. The service layer can be seen as the various internet service platforms that people use to search for information, conduct networking, or engage in communication. The cognitive layer involves human actors who are driven by both cognitive and psychosocial stimuli.

Several countries have published national cybersecurity strategies that include definitions of the key terms and concepts of cybersecurity (Committee, Secretariat of Security, 2019; Sabillon et al., 2016; Shafqat & Masood, 2016). Finland's first cybersecurity strategy was published in 2013 and provided definitions of key terms in the field (Committee, Secretariat of Security, 2013). The terms and their relationships and interdependences were specified in more detail in the 2018 Glossary of Cybersecurity (TSK, 2018). According to the Glossary of Cybersecurity (translated from Finnish into English by the author):

> Cybersecurity is a target state in which the cyber operating environment can be trusted and where its operation is secured (TSK, 2018).

It was also noted that:

> Cybersecurity includes actions to proactively manage and, where necessary, tolerate various cyber threats and their impacts. Disruption of the cyber environment is often caused by a realised security threat, so information security is a key factor in the pursuit of cybersecurity. In addition to information security, cybersecurity is pursued, among other things, through actions aimed at securing the functions of the physical world that depend on a disrupted cyber environment. Whereas information security refers to the availability, integrity, and confidentiality of information, cybersecurity refers to the security of a digital and networked society or organisation and the impact of a member on its operations (TSK, 2018).

The glossary distinguishes between cybersecurity and information security and defines their connection to each other. Today, cybersecurity is a recognised discipline and concept (Dhawan et al., 2020). Security demands in the information technology (IT) sector have traditionally focused on data security. Digital operating environments have evolved to encompass almost all human activities, in both working life and leisure. This development has resulted in the emergence of many security threats either through or in the digital environment (Humayun et al., 2020; Luiijf, 2012; Vähäkainu et al., 2020).

2.2 Cybersecurity education

Changes in operational principles in society and on the global stage can also be reflected in the necessity to change learning content and learning methods. Cybersecurity has evolved into one of the most important content areas in the field of ICT education (Carayannis et al., 2018; Dawson & Thomson, 2018). Competency needs relating to cybersecurity are derived from those required for information security. Within cybersecurity, several functionalities can be distinguished, which in themselves form specific areas of expertise (Nyre-Yu, 2021, Roy et al., 2020). Alongside these new competency requirements, the educational needs for competency development have also changed. Over the past 10 years, university degree programmes have begun to include cybersecurity options (Lehto, 2020; Parrish, 2018; Skirpan, 2018). Cybersecurity as a discipline is traditionally understood as a technical area in which various technical controls are used to protect IT architecture and ensure that unauthorised users are not able to penetrate the infrastructure without permission. Another technical aspect relates to so-called penetration testing, and a third aspect considers secure programming. These technical emphases are commonly reflected in cybersecurity education (Jones, 2018; Kazemi, 2010; Tabassum, 2018). According to literature reviews concerning cybersecurity education, when the human aspects are covered in educational programmes, they include privacy, social engineering, law, ethics, and social impacts (Skirpan, 2018; Švábenský, 2020).

The ICT industry has traditionally been understood as rapidly evolving (Dinevski & Kokol, 2004). Due to technical development, the need to update competencies continues throughout a person's career. For lifelong learning and continuing education to remain relevant for working life, educational environments must reflect realistic working environments and enable competencies to be used in practice. Complex ICT architectures demand complex requirements for educational platforms. Educational planning for lifelong learning must be agile to meet the needs of working life, and modern training platforms make it easy for developers to design content for the users of new technologies.

2.3 Cyber security exercises

A long tradition exists of using laboratory environments for engineering training (Abdulwahed & Nagy, 2011; Chou & Feng, 2019; Jin, 2018; Lal et al., 2020). Laboratory environments allow students to practice and apply theory (Nordio et al., 2010; Sevgi, 2003). Traditional ICT laboratory environments model a particular functionality or part of it, thus enabling students to practice their skills in a modelled environment (Linn, 2011; Xu et al., 2013). The cybersecurity sector often combines the phenomena of several technical areas into functional processes, forming technical–functional entities, the operation and cause-and-effect relationships of which ought also to be incorporated into teaching and skills acquisition (Davis & Magrath 2013). Cybersecurity laboratory environments constructed as learning/training environments are commonly referred to as cyber ranges (Ferguson et al., 2014; Pham et al., 2016; Vykopal et al., 2017).

There are several forms of cybersecurity training and exercises. The goals of the different training methods differ, and the training methodologies develop over time. The following four different methods are the most commonly used training methods today. A Capture the Flag (CTF) exercise is often a competitive, partially or entirely game-based form of exercise, in which students search for environmental signs that guide them towards the learning goals of the exercise (Taylor et al., 2017; Vigna et al., 2014). A digital forensic incident response (DFIR) exercise is typically conducted with infrastructure modelled on the exercise platform to enable students to locate a potential breach and/or evidence of a breach (Moser & Cohen, 2013; Park et al., 2019). Tabletop exercises are a traditional way to practice skills, especially business management skills, using cases to mirror possible responses to set chains of events (Angafor et al., 2020; Dausey et al., 2007). The final type is the live exercise, which is the subject of this study. A live exercise is performed on a training platform in which the situation changes according to a pre-planned scenario. The exercise typically involves an exercise management team, also known as a white team (WT), a red team (RT) that simulates the actions of a threat actor, and a blue defending team (BT) that protects the given infrastructure. A green team (GT) can also be set up to handle the functionality of the training platform, while a purple team (PT) is responsible for acting as a research team and monitoring the teams' actions regarding any research and/or development goals (Doupé et al., 2011; Geers, 2010; Kick, 2014; Kim et al., 2019).

The digital cybersecurity learning environment of Jyväskylä University of Applied Sciences was used as the research environment for this study. The learning environment is called the realistic global cyber environment (RGCE), and the structure of the learning environment and its pedagogical attributes were examined in this research.

3 RESEARCH METHODS AND DATA

3.1 Research approach

According to the original research plan, this study collected quantitative data and used quantitative research methods to study learning in cybersecurity exercises. After the first sampling of the quantitative data, it became evident that quantitative data alone would not be able to explain learning and the related requirements of the learning environment to an adequate degree. Thus, elements of qualitative research were added to complement the study. In its entirety, the study combines elements of quantitative and qualitative research.

3.1.1 Mixed methods

Overall, the research adopted a mixed-methods research methodology. Mixed-methods research is a research approach that utilises both quantitative and qualitative research methods at different stages of the research to ensure, for each stage of the research or each research question, the use of the research method that best answers the research question (Tashakkori et al., 2020; Hurmerinta-Peltomäki & Nummela, 2006; Johnson et al., 2004; Tashakkori et al., 1998). Traditionally, the mixed-methods approach has been adopted in business studies, the behavioural sciences, and sociology (Tashakkori et al., 1998). Mixed-methods research has the benefit of combining several disciplines to ensure research effectiveness (Mäses et al., 2019; Molina-Azorin, 2012; Rege et al., 2017).

The objective of combining research methods is to generate a more in-depth understanding of the research subject (Clark et al., 2008; Rossman & Wilson, 1985). In this study, the combination of research methods facilitated an abductive and iterative deepening of understanding (Van Maanen et al., 2007) to enable quantitative data to be employed for the basic statistical analysis of the phenomenon under study. Concerning learning in an exercise, quantitative data can show that the exercise facilitates new competencies for the student. Qualitative research identifies elements that have supported learning, such as requirements for the teaching environment, the pedagogical methodology relating to the life cycle of the exercise, a picture of the key elements of the exercise constructed through the experience of the teacher, and their relevance to learning. Thus, research methods and the data they produce may partially overlap and can be modelled in many ways according to different research approaches and paradigms (Shannon-Baker, 2016).

3.1.2 Constructive research approach

Articles II, III, IV, V, VII, and VIII explained the methodology of the traditional constructive research approach. The research method has become more common, especially in the fields of technology, information systems science, and educational science (Dodig-Crnkovic, 2010; Kasanen, 1993; Lehtiranta et al., 2016).

A constructive research approach typically considers a research object such as a model, process, plan, information system model, or organisational structure using an iterative process to develop a construct that provides a new solution to a problem or deviates from and/or broadens the existing interpretation (Lukka & Tuomela, 1998). A constructive research approach is characterised by an empirical intervention that aims to produce a new interpretation or new information about a research subject (Keating, 1995; Lukka, 2000). A commonly identified problem with the constructive research approach is a possible lack of objectivity on the part of the researcher (Norris, 1997). To reduce this error, the researcher should expose the research set-up to evaluation by an external party or use peer review to obtain a qualitative perspective and verify the research process.

3.1.3 Qualitative interviews

Interviews leading to qualitative content analysis were used for Articles VI and IX.

The research approach involved semi-structured interviews with experts (Hirsjärvi & Hurme, 2008), the aim of which was to deepen the researcher's understanding of the elements of cybersecurity exercises and provide more detailed information to underpin the statistical analyses. The interviews were based on a general interview framework which enabled the interviews to be conducted in a way that allowed interviewees to associate freely with a generic question. Hence, the interviews combined questions with different scopes in an attempt to obtain sufficiently detailed information about the subject under study (Saaranen-Kauppinen & Puusniekka, 2009).

3.1.4 Quantitative analysis

It was intended at the design stage of the research to collect and use quantitative data in the study. A quantitative study approach can produce comparative data that is fundamental to the subject of the study and can be used as base information in later stages of the study (Martyn, 2008; Woodley, 2004). A quantitative approach was used for Articles III and VI.

Data was collected from a cybersecurity exercise organised as part of a degree-level cybersecurity exercise. The aim of the quantitative analysis was to examine the competency development experienced by the students who participated in the cybersecurity exercise. A questionnaire was prepared to measure the development of cybersecurity competencies. Surveys were conducted with two samples, and the responses were analysed using statistical methods.

3.2 Data collection

The articles for these studies provided an overall picture and understanding of the pedagogical principles of cybersecurity training, learning during the exercises, and the pedagogical requirements of the training platform. Table 1 summarises the articles and the research methods used in them and outlines the contributions of the articles to this dissertation.

TABLE 1. Data collection methods and article contributions to the dissertation

Article	Methods	Focus and contribution
I	Literature review.	A review of the existing research regarding simulation learning, collaborative learning, and game-based learning.
II	Expert evaluations of learning methods and models, and a constructive research approach.	Pedagogical aspects of cybersecurity exercises.
III	Expert evaluations and structuring of the questionnaire. Constructive research approach. Survey of students engaging in cyber security exercise using descriptive statistical analysis.	NIST NICE framework-based questionnaire and learning in an on-site cybersecurity exercise.
IV	Expert evaluations of learning methods and models for the structured model. Constructive research approach.	Pedagogical requirements for a comprehensive cyber arena. Development of the cyber arena model.
V	Expert evaluations of learning methods and models. Constructive research approach.	Pedagogical principles of cybersecurity exercises and assessment of the exercise.
VI	Survey of students engaging in an on-line cybersecurity exercise using descriptive statistical analysis. Qualitative interviews with lecturers using conventional content analysis.	Measuring learning in on-line cybersecurity exercise. Developing a collaboration platform for an online exercise.

Article	Methods	Focus and contribution
VII	Expert evaluations of learning methods and models. Constructive research approach.	Curriculum building based on an existing NIST NICE framework.
VIII	Expert evaluations of learning methods and models. Constructive research approach.	Heuristic model for developing a degree education curriculum.
IX	Qualitative interviews with lecturers followed by conventional content analysis.	Research regarding an authentic learning environment for in-service training in cybersecurity.

4 RESEARCH CONTRIBUTION

This article-based study carried out by the author consisted of designing the research settings, considering the practical implementation of the research, and analysing the research results in collaboration with other researchers who had participated in the research publications.

Article I described a traditional literature review that sought to clarify, based on previous publications, what type of pedagogical principles had been used in various professional studies to underpin virtualised or simulated teaching environments. The aim of the article was to gather basic information about pedagogical models that could be utilised at a later stage of the research to build a pedagogical framework for cybersecurity training. The keywords through which the literature review was conducted were game-based learning, simulation learning, and collaborative learning. The study showed that pedagogical models, according to the keywords, were quite widely used in various substantive areas. However, the findings also indicated that there was virtually no applied research on pedagogical models and principles for cybersecurity training. The work of the author for the publication included literature searches, article analyses, and writing the article as the second author.

For Article II, a pedagogical model was developed for the pedagogical principles of cybersecurity training. The knowledge base of the model related to the organisation of cybersecurity exercises and learning mechanisms in exercises organised by Jyväskylä University of Applied Sciences during 2013–2019. The authors of the article participated in cybersecurity exercises organised during the mentioned years, along with 1,500 other people. The work of the author for the article included the design of the structure, content, and analysis of the article, as well as the design of the constructed pedagogical model and writing the paper, for which the author was the main author.

For Article III, a set of questions was designed to measure the level of competence of a person participating in a cybersecurity exercise both before and after the exercise. The set of indicators was based on the generally accepted and widely used NIST NICE framework and cybersecurity model (Newhouse et al., 2017). A questionnaire was distributed in an exercise organised using an onsite method in spring 2019. The author participated in the design of the questionnaire, the construction of the research sample, and the analysis. The author was the main author of the article.

For Article IV, pedagogical requirements were defined for the comprehensive cyber arena model, necessitating a modern digital operating environment underpinned by authentic learning environment theory. The author participated in the design of the model and the definition of pedagogical requirements. The author was the main author of the article.

For Article V, the pedagogical model developed for Article II was expanded upon and the content of the model was clarified, especially regarding the assessment of a student participating in a cybersecurity exercise. The author designed the structure of the paper and the expansion of the pedagogical model. The author was the main author of the paper.

For Article VI, a second sample completed the questionnaire constructed in Article III in spring 2020. The participants engaged in an online exercise. The article described a general model for creating a collaborative learning context for an online exercise. The author designed the structure of the article and the research methods and participated in the collection and analysis of the research data. The author was the main author of the article.

Article VII addressed the testing and evaluation of the existing NICE NIST competency framework for constructing a curriculum. The author participated in analysing the framework and designing the created model. The author acted as the second author of the article.

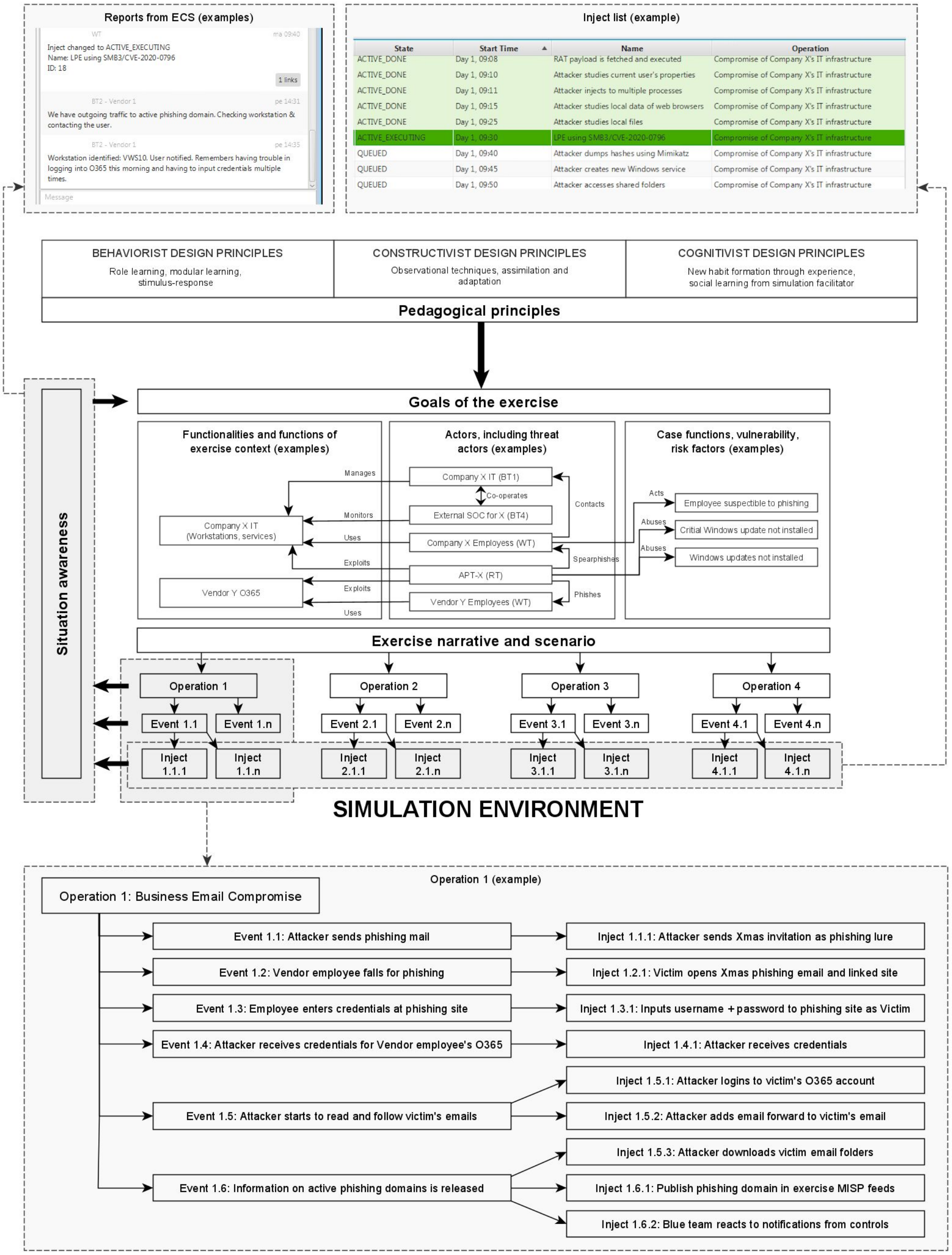
Article VIII examined the ICT sector and constructed a curriculum for emerging technologies using a heuristic model. The researcher designed the heuristic approach and participated in the construction and analysis of the model. The author acted as the second author of the article.

Article IX examined the specific features of the content of the cybersecurity exercise offered as in-service training and their implementation in the exercise. The researcher participated in the preparation of the research plan and the analysis of the research data. The author was the main author of the paper.

4.1 Pedagogical principles of cybersecurity exercises (Articles I, II, and V)

As part of the research, the pedagogical principles underpinning cybersecurity exercises were examined. Previous studies have seldom evaluated how the pedagogical principles of cybersecurity exercises are constructed, what elements the principles cover, and how they should be used to support a practical exercise.

The pedagogical principles identified in the study are shown in Figure 1. At the top of the figure are the pedagogical theories, the application of which underpinned the pedagogical aspects of the exercise. Learning theories must be comprehended as the descriptive parts of teaching methods that make up the whole. The behaviourist theory of learning was adopted to examine how certain basic competencies were developed. Role playing is a practice often used in simulation environments to allow students to practice tasks or roles assigned to them. Learning is modular (modular learning), and the competency development of students is facilitated by events, in response to which students are guided towards set learning goals (Tynjälä & Collin, 2000).



Reports from ECS (examples)

WT ma 09:40
Inject changed to ACTIVE_EXECUTING
Name: LPE using SMB3/CVE-2020-0796
ID: 18
1 links

BT2 - Vendor 1 pe 14:31
We have outgoing traffic to active phishing domain. Checking workstation & contacting the user.

BT2 - Vendor 1 pe 14:35
Workstation identified: VWS10. User notified. Remembers having trouble in logging into O365 this morning and having to input credentials multiple times.

Message

Inject list (example)

State	Start Time ▲	Name	Operation
ACTIVE_DONE	Day 1, 09:08	RAT payload is fetched and executed	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:10	Attacker studies current user's properties	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:11	Attacker injects to multiple processes	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:15	Attacker studies local data of web browsers	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:25	Attacker studies local files	Compromise of Company X's IT infrastructure
ACTIVE_EXECUTING	Day 1, 09:30	LPE using SMB3/CVE-2020-0796	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:40	Attacker dumps hashes using Mimikatz	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:45	Attacker creates new Windows service	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:50	Attacker accesses shared folders	Compromise of Company X's IT infrastructure

BEHAVIORIST DESIGN PRINCIPLES
Role learning, modular learning, stimulus-response
CONSTRUCTIVIST DESIGN PRINCIPLES
Observational techniques, assimilation and adaptation
COGNITIVIST DESIGN PRINCIPLES
New habit formation through experience, social learning from simulation facilitator
Pedagogical principles
Situation awareness
Goals of the exercise
Functionalities and functions of exercise context (examples)
Actors, including threat actors (examples)
Case functions, vulnerability, risk factors (examples)
Manages
Monitors
Uses
Exploits
Exploits
Uses
Company X IT (Workstations, services)
Vendor Y O365
Company X IT (BT1)
Co-operates
External SOC for X (BT4)
Company X Employess (WT)
APT-X (RT)
Vendor Y Employees (WT)
Contacts
Spearphishes
Phishes
Acts
Abuses
Abuses
Employee suspectible to phishing
Critial Windows update not installed
Windows updates not installed
Exercise narrative and scenario
Operation 1
Operation 2
Operation 3
Operation 4
Event 1.1
Event 1.n
Event 2.1
Event 2.n
Event 3.1
Event 3.n
Event 4.1
Event 4.n
Inject 1.1.1
Inject 1.1.n
Inject 2.1.1
Inject 2.1.n
Inject 3.1.1
Inject 3.1.n
Inject 4.1.1
Inject 4.1.n
SIMULATION ENVIRONMENT
Operation 1 (example)
Operation 1: Business Email Compromise
Event 1.1: Attacker sends phishing mail
Inject 1.1.1: Attacker sends Xmas invitation as phishing lure
Event 1.2: Vendor employee falls for phishing
Inject 1.2.1: Victim opens Xmas phishing email and linked site
Event 1.3: Employee enters credentials at phishing site
Inject 1.3.1: Inputs username + password to phishing site as Victim
Event 1.4: Attacker receives credentials for Vendor employee's O365
Inject 1.4.1: Attacker receives credentials
Inject 1.5.1: Attacker logins to victim's O365 account
Event 1.5: Attacker starts to read and follow victim's emails
Inject 1.5.2: Attacker adds email forward to victim's email
Inject 1.5.3: Attacker downloads victim email folders
Event 1.6: Information on active phishing domains is released
Inject 1.6.1: Publish phishing domain in exercise MISP feeds
Inject 1.6.2: Blue team reacts to notifications from controls

FIGURE 1. The pedagogical principles of cybersecurity exercises

The behavioural learning methodology used in the model reflected the basic competencies of students, using simple exercises (Sahlberg & Leppilampi, 1994). Based on the cognitive learning methodology, the model highlighted experiential learning. According to the theory of cognitive learning, students should also be provided with a social environment that supports individual learning (Efland, 1995; Merriam 2004; Nevgi & Lindblom-Ylänne, 2003). Based on the constructive conception of learning, the model highlighted the ability of students to observe events in an operating environment, decide their own actions in response to the environment and other actors, assimilate de facto technological principles and general standards, and function as actors (Rauste-von Wright & von Wright, 1996; Siemens & Conole, 2011). Thus, an upper part of Figure 1 reflects the different levels of competence and skills of learners, starting with the basic concepts of teaching and learning and ending with the voluntary activity of learners in a learning environment simulating a realistic environment in which an individual acts as a part of a group and reflects on the effectiveness of his/her own responses with peers in the group.

In the case of a university student or an adult learner in in-service training, it is imperative that andragogic principles are taken into account in pedagogical planning (Knowles, 1995). An adult learner has a previous knowledge base on which to construct new learning and, in a learning situation, is often able to apply existing skills or the experiences he/she has gained either through previous study or in working life (Merriam & Bierema, 2013). It is often the case that former learning, or an understanding of how, for example, a technical workflow needs to be performed, may hinder or slow down the learning of something new. The learner should be able to build cognitive dissonance, which guides him/her to adopt a new way of working. For the above, the activity should be implemented in such a way that the learner is able to reflect on the previous activity, and the learning environment should be as close to reality as possible in its functionalities (Knowles, 1995).

According to experiential learning theory, experience alone does not guarantee good learning outcomes. The learner must have opportunities to reflect on the learning experience, both with peer learners and teachers (Kolb et al., 2001). When a learner expresses his or her own learning experience through speech or writing, he/she simultaneously structures new knowledge and forms a new construction of understanding (Laal, 2013). In his theory of deliberate practice, Ericsson argued that the use of a specific learning environment is essential in building new expertise for experts (Ericsson, 2008). When competence is already at a high level for the learner, special attention must be paid to defining learning objectives so that the environment adequately supports learning. The model of levels of competence built by Miller also supported this argument, and competence should ideally be at the highest level of the Miller pyramid (Miller, 1990).

A cybersecurity exercise is a suitable learning tool, especially for students who already have some knowledge of cybersecurity. If there is no basic competence, the learning events modelled in the learning environment will remain detached or will not be noticed by the learners. The objectives of a competency development exercise should be established according to general pedagogical principles. For goal setting, it is especially necessary to consider the level of competence of the training group, thus ensuring realistic achievement of the desired level of competence. In practice, an exercise scenario sets the frame of reference in which learning is acquired. The life cycle of an exercise begins with the design of an exercise scenario, which then defines the intended learning objectives.

4.1.1 Collaborative learning

Collaborative learning theory is one of the most essential components of pedagogical thinking in cybersecurity practice. A key element of a cybersecurity exercise is individuals acting as a team. Team-oriented exercises simulate commonly used real-life functions, such as those in a security operations centre (SOC), a network operations centre (NOC), or an incident response team. These functionalities are commonly used in the field of cybersecurity and are organised to enable learners to perform the control and/or response tasks assigned to them. It is widely understood that the maintenance and control of a large architecture requires a team set-up, since one individual alone cannot control the architecture 24/7 or have the ability to embrace all the technological aspects. Thus, it is natural that learning situations are used as pedagogical tools in lectures, enabling individuals to learn to act as part of a team, in addition to developing competence in the subject.

In community learning, a group of actors builds a collective comprehension of the object of action through collaboration, and participants thereby learn as part of a team (Panitz, 1999). Team members are responsible for their own tasks or roles, through which they construct their own learning experiences by problem solving, completing tasks, and sharing their experiences with other members of the group. Individuals receive support, help, and insights from their peers, thus enabling the group to progress towards the set learning goals (Laal, 2013). According to the pedagogical principles of cybersecurity exercises, community learning is manifested in the operations of a planned scenario, which are carried out in the learning environment based on an exercise plan. Operations are targeted towards one or more teams that are responsible for their own infrastructure. Operations are divided into events and inputs, which in practice target the IT infrastructure modelled in the training environment. By responding to events and inputs, teams perceive, identify, and manage the situation, and learners thus build their own learning experience and contribute as part of a group to the collective learning of the entire group.

4.1.2 Simulation pedagogy

A long tradition of simulation pedagogy exists, especially in the nursing and medical education sectors (Bariran et al., 2013; Emin-Martinez & Ney, 2013; Kalaniti & Campbell, 2015; Nyström et al., 2016). Engineering has also been traditionally viewed as an important field in which simulation adds value by enabling learners to practice hands-on skills or technical configurations. As operating environments have become more complex, the technical field has increasingly shifted from traditional laboratory environments to modelled simulation learning environments (Debatty & Mees, 2019; European Defence Agency, 2018; Pridmore et al., 2010).

In the field of cybersecurity, special attention must be paid to the security of the teaching environment. Creating genuine malware or vulnerabilities in the operating environment is often not possible in so-called open or production environments. The simulated environment offers experts a special opportunity to practice activities that involve a high level of risk, as well as to learn to identify genuine malware and anomalies in operating environments. Constructing a simulation environment is expensive, so optimising the learning environment is imperative because it sets the boundary conditions for learning and the simulated environment. In the pedagogical model of a cybersecurity exercise, the simulation environment is constructed from a set of IT architectures embedded into the environment, as well as a scenario constructed for the pedagogical objectives of the exercise and the operations, tasks, and inputs that support it.

4.1.3 Authentic learning environments

Herrington and Oliver defined the requirements for a realistic learning environment based on authentic learning environment theory (Herrington & Oliver, 2000). According to Herrington and Oliver (2000), the learning environment should embody similar elements and functionalities to those that learners encounter when applying their learning in real working life.

The requirements for a learning environment that simulates a real situation according to their theory are as follows:

1. Provide an authentic context that describes or corresponds to the way in which knowledge and skills are used in real life.
2. Provide authentic activities that can be the main content of the whole course or study unit.
3. Provide learners with models of how to actually perform in real-life situations.
4. Enable and encourage learners to take on different roles, consider what they are learning, and experience the learning environment from different perspectives.
5. Provide opportunities for collaborative knowledge creation.
6. Provide opportunities for learners to reflect on their levels of competence and learning regarding the context of the learning environment, authentic tasks, and expertise.
7. Provide opportunities for students to articulate and justify their actions and choices to others.

8. Provide students with community support for the learning process that does not oversimplify the learning environment but prepares and creates support structures for people to do things in a meaningful way.
9. Tightly integrate the assessment of learning into activities and allow learners to focus on activities and learning and to produce products and outputs in collaboration with others.

In addition to the design requirements for a learning environment, the pedagogical exercises and tasks carried out in the learning environment should be designed according to authentic learning theory (Herrington, 2006).

4.2 Learning in a cybersecurity exercise (Articles III and VI)

Cybersecurity exercises have become an established part of cybersecurity training, both in degree-level education and in-service training. A cyber arena, which serves as a cybersecurity teaching environment, can be used in degree-level education as a teaching environment to replace a traditional laboratory environment. A cyber arena facilitates training for large entities, as well as the simulation of sub-entity interoperability, which must be viewed as a significant advantage over traditional laboratory environments. However, little research has examined the effectiveness of cybersecurity exercise as a pedagogical teaching method (Ernits et al., 2020; Hoffman et al., 2005). The aim of the studies was to develop and test a set of indicators by which learning in cybersecurity exercises could be measured.

4.2.1 Questionnaire for learning evaluation

The NIST NICE Cybersecurity Competence Framework, which has been widely adopted by industry and with high-level recognition, was selected as the basis for the questionnaire (Newhouse et al., 2017). The NIST NICE framework identifies a total of 630 knowledge components. In the first phase, experts reviewed the framework so that only the most important aspects of cybersecurity were included in the question battery, enabling learning to be measured in cybersecurity exercises. Five cybersecurity experts reviewed the NIST NICE knowledge components, and each identified the areas they believed should be covered in the question battery. Knowledge components that received at least four mentions were then reviewed and modified to eliminate overlaps, leaving a total of 44 final questions:

1. Cyber threats and vulnerabilities
2. Organization's enterprise information security and architecture
3. Resiliency and redundancy
4. Host / network access control mechanisms
5. Cybersecurity and privacy principles
6. Vulnerability information dissemination sources

7. Incident categories, incident responses, and timelines for responses
8. Incident response and handling methodologies
9. Insider Threat investigations, reporting, investigative tools and laws/regulations
10. Hacking methodologies
11. Common attack vectors on the network layer
12. Different classes of attacks
13. Cyber attackers
14. Confidentiality, integrity, and availability requirements and principles
15. Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications
16. Network traffic analysis (tools, methodologies, processes)
17. Attack methods and techniques (DDoS, brute force, spoofing, etc.)
18. Common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)
19. Malware
20. Security implications of software configurations
21. Computer networking concepts and protocols, and network security methodologies
22. Laws, regulations, policies and ethics as they relate to cybersecurity and privacy
23. Risk management processes (e.g. methods for assessing and mitigating risk)
24. Cybersecurity and privacy principles
25. Specific operational impacts of cybersecurity lapses
26. Authentication, authorization, and access control methods
27. Application vulnerabilities
28. Communication methods, principles, and concepts that support the network infrastructure
29. Business continuity and disaster recovery continuity
30. Local and Wide Area Network connections
31. Intrusion detection methodologies and techniques for detecting host or network -based intrusions
32. Information technology security principles and methods (e.g. firewalls, demilitarized zones, encryption)
33. Knowledge of system and application security threats and vulnerabilities
34. Network traffic analysis methods
35. Server and client operating systems
36. Enterprise information technology architecture
37. Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
38. System administration, network, and operating system hardening techniques
39. Risk/threat assessment

40. Knowledge of countermeasures for identified security risks. Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
41. Packet-level analysis using appropriate tools (e.g. Wireshark, tcpdump)
42. Hacking methodologies
43. Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
44. Methods and techniques used to detect various exploitation activities

For each of the 44 questions, five competency-level questions were presented to participants to determine whether they felt that they had encountered the cybersecurity component during the exercise:

1. (Topic) was/were presented in the exercise. [Yes/No]
2. (Topic) was/were something I personally encountered during the exercise. [Yes/No]
3. My knowledge of (topic) increased during the exercise. [Yes/No]
4. Level of knowledge before the exercise. [1–10]
5. Level of knowledge after the exercise. [1–10]

A scale of 1–10 was selected as the scale for measuring their own levels of competence, which was performed both before and after the exercise. The scale ranged from 1 (no knowledge) to 10 (expert knowledge). The reason for this wide scale was to ensure that the respondents could identify their levels of competence precisely, both before and after the exercise. Too narrow a scale might have resulted in some knowledge acquisition going unnoticed. The survey was built into a Webropol environment and was made available to students immediately after the exercise in spring 2019.

4.2.2 Learning in the on-site exercise

The questionnaire respondents were undergraduate students at Jyväskylä University of Applied Sciences, for whom the cybersecurity exercise was part of the cybersecurity module in the curriculum. The exercise was organised on the premises of the university as an on-site exercise. All the activities in the exercise were conducted in a single physical location, where each team had its own classroom. The information systems, communication connections, and tools requested by the teams were provided in each classroom. The exercise used a comprehensive cyber arena-style learning platform owned by Jyväskylä University of Applied Sciences. Answering the questionnaire was voluntary for the students, and instructions for answering were given during the course. The survey was distributed through Webropol to 53 students, of whom 21 answered all the questions. Figure 2 shows the response data depicted as a box plot diagram. In the figure, the red box plot depicts the knowledge level of a student for the sub-area pre-exercise, while the blue box plot indicates the knowledge level identified post-exercise.

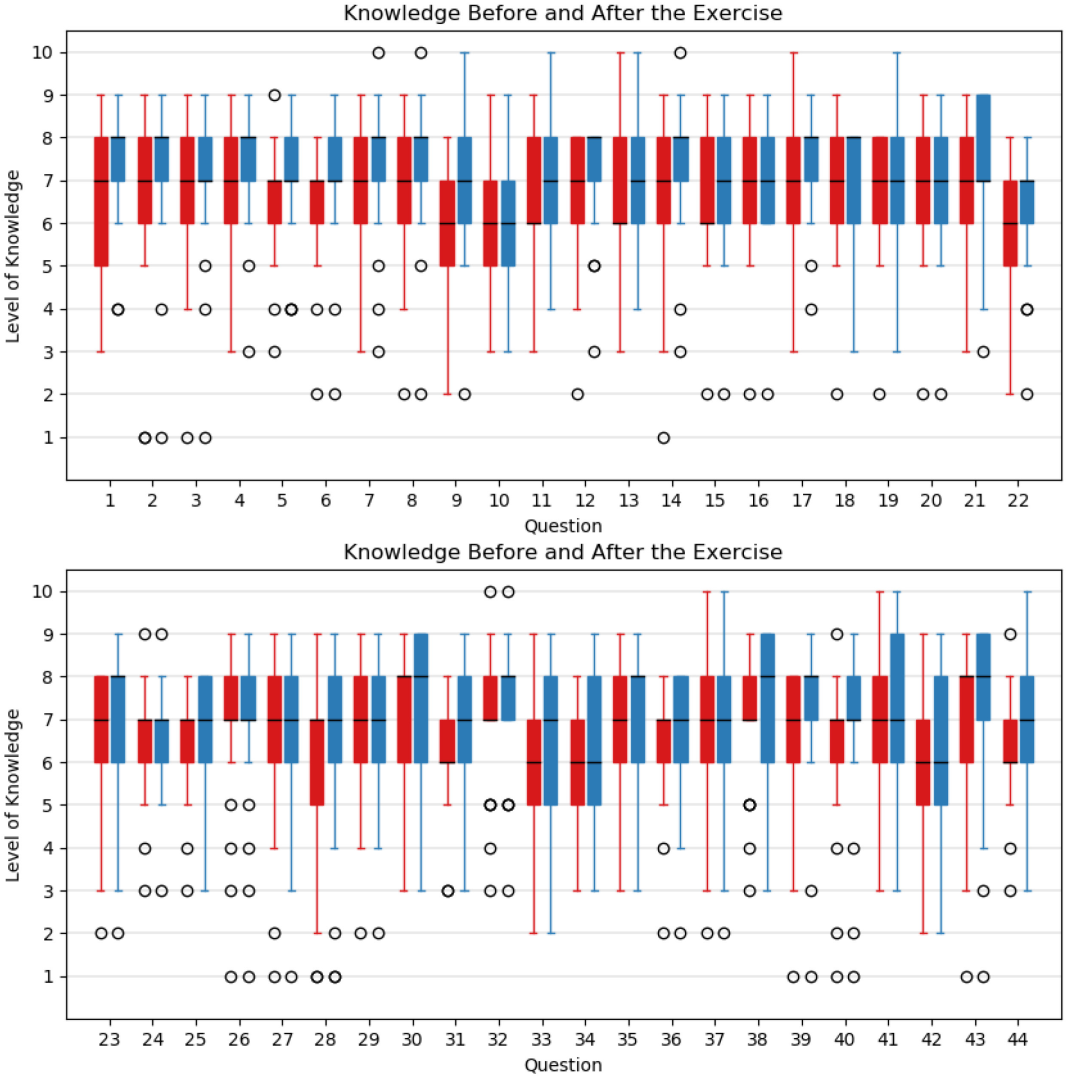


FIGURE 2. Level of knowledge before (red) and after (blue) the on-site exercise

Due to the relatively small number of responses, the results needed to be analysed with the following guidance. The before/after competency levels shown in Figure 2 are averages of the scores for each question. The presentation based on averages was chosen because, when the sample is small, the median may fail to indicate a change in the sample. However, based on the data, it can be confidently stated that in 36 of the 44 areas, the level of competence increased significantly during the exercise. A total of 53 students started answering the questionnaire, but only 21 students completed it. Hence, it could be concluded that the questionnaire containing five questions for each of the 44 areas was too long and/or too detailed for the students, leading to some respondents omitting responses.

Based on the results, it was clear that the NIST NICE framework was an appropriate basis for a questionnaire intended to measure levels of competence. The detailed nature of the question set allowed questions to be directed towards a specific area of cybersecurity expertise.

4.2.3 Learning in the online exercise

According to the original research plan, the 2019 research sample presented in the previous chapter was to be supplemented with a new sample in spring 2020, thus providing a larger number of responses to verify learning in an on-site cybersecurity exercise. When the cybersecurity exercise started in the winter of 2020 according to the curriculum, only one contact was organised from the contact times preparing for the exercise according to the plan. Due to the coronavirus epidemic beginning in March 2020, the exercise could not be organised as an on-site exercise as planned. Therefore, the exercise was converted into an online exercise. To organise the exercise according to the pedagogical principles presented in this study, the online exercise had to provide a collaboration platform that supported collaborative learning.

Figure 3 shows the collaboration platform constructed for the online exercise, which allowed students to work in teams according to collaborative learning theory, even though the exercise was conducted online. For scheduling reasons, the communication platform was built on top of the Microsoft Team platform. Another option would have been to construct the communication from the beginning entirely inside the cyber arena, which, however, was not possible due to schedule restrictions. The Microsoft Teams platform was used for voice communication and video sharing, for example, in situations where a student carried out a demanding technical action and wanted to share the workflow with all team members. Also, files and Excel spreadsheets were shared on the platform. Team-specific voice channels were established to support each team's platform. The Gitlab environment was adopted for the course assignments and the sharing of general material. In the cyber arena environment, students had a VPN tunnelled connection that allowed them to join and use the cyber arena normally through the VMware CloudDirectory.

The online arrangements enabled the exercise to be conducted under conditions like those used for the 2019 research sample. The use of the cyber arena involved a second research sample completing the 2019 questionnaire. Because the samples differed in terms of student participation, the sample responses did not coincide with the 2019 sample, but the data were treated as a separate sample for the online cybersecurity exercise to measure competency development.

In addition to the questionnaire described, qualitative interviews were conducted with three members of staff who supervised the exercise. Interviews were analysed using traditional qualitative content analysis (Hsieh & Shannon, 2005a). The aim of the interviews was to examine the implemented online training arrangements and their functionality from the point of view of the teaching staff. The interviews also sought to gather the views of experienced teachers regarding the success of the online exercise and its usefulness as a training method.

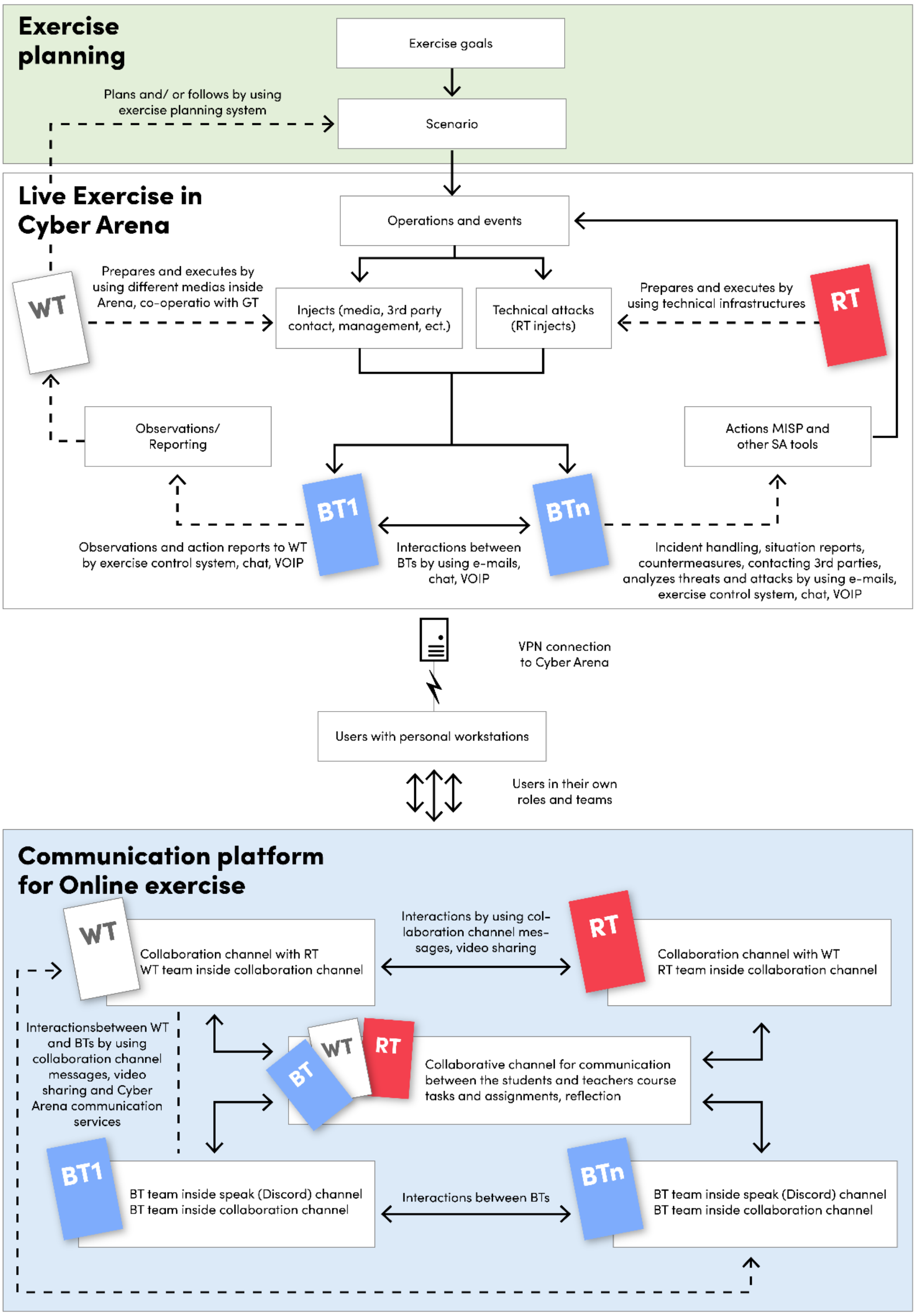

Exercise planning
Exercise goals
Plans and/ or follows by using exercise planning system
Scenario
Live Exercise in Cyber Arena
Operations and events
WT
Prepares and executes by using different medias inside Arena, co-operatio with GT
Injects (media, 3rd party contact, management, ect.)
Technical attacks (RT injects)
Prepares and executes by using technical infrastructures
RT
Observations/ Reporting
Actions MISP and other SA tools
BT1
BTn
Observations and action reports to WT by exercise control system, chat, VOIP
Interactions between BTs by using e-mails, chat, VOIP
Incident handling, situation reports, countermeasures, contacting 3rd parties, analyzes threats and attacks by using e-mails, exercise control system, chat, VOIP
VPN connection to Cyber Arena
Users with personal workstations
Users in their own roles and teams
Communication platform for Online exercise
WT
Collaboration channel with RT
WT team inside collaboration channel
Interactions by using collaboration channel messages, video sharing
RT
Collaboration channel with WT
RT team inside collaboration channel
Interactionsbetween WT and BTs by using collaboration channel messages, video sharing and Cyber Arena communication services
BT
WT
RT
Collaborative channel for communication between the students and teachers course tasks and assignments, reflection
BT1
BT team inside speak (Discord) channel
BT team inside collaboration channel
Interactions between BTs
BTn
BT team inside speak (Discord) channel
BT team inside collaboration channel

FIGURE 3. Collaboration platform for the online exercise

The survey was conducted using the same questions as in 2019. Responding to the questionnaire was included in the course requirements of the curriculum and therefore a 100% completion rate was achieved. Since the total sample size was relatively small, a decision was made to analyse the data based on the calculated averages. Means, medians, standard deviations, and p-values were calculated, and the aim was to ensure that the results were not distorted by, for example, skewed distribution. Figure 4 shows the data collected from the online exercise as a box plot diagram.

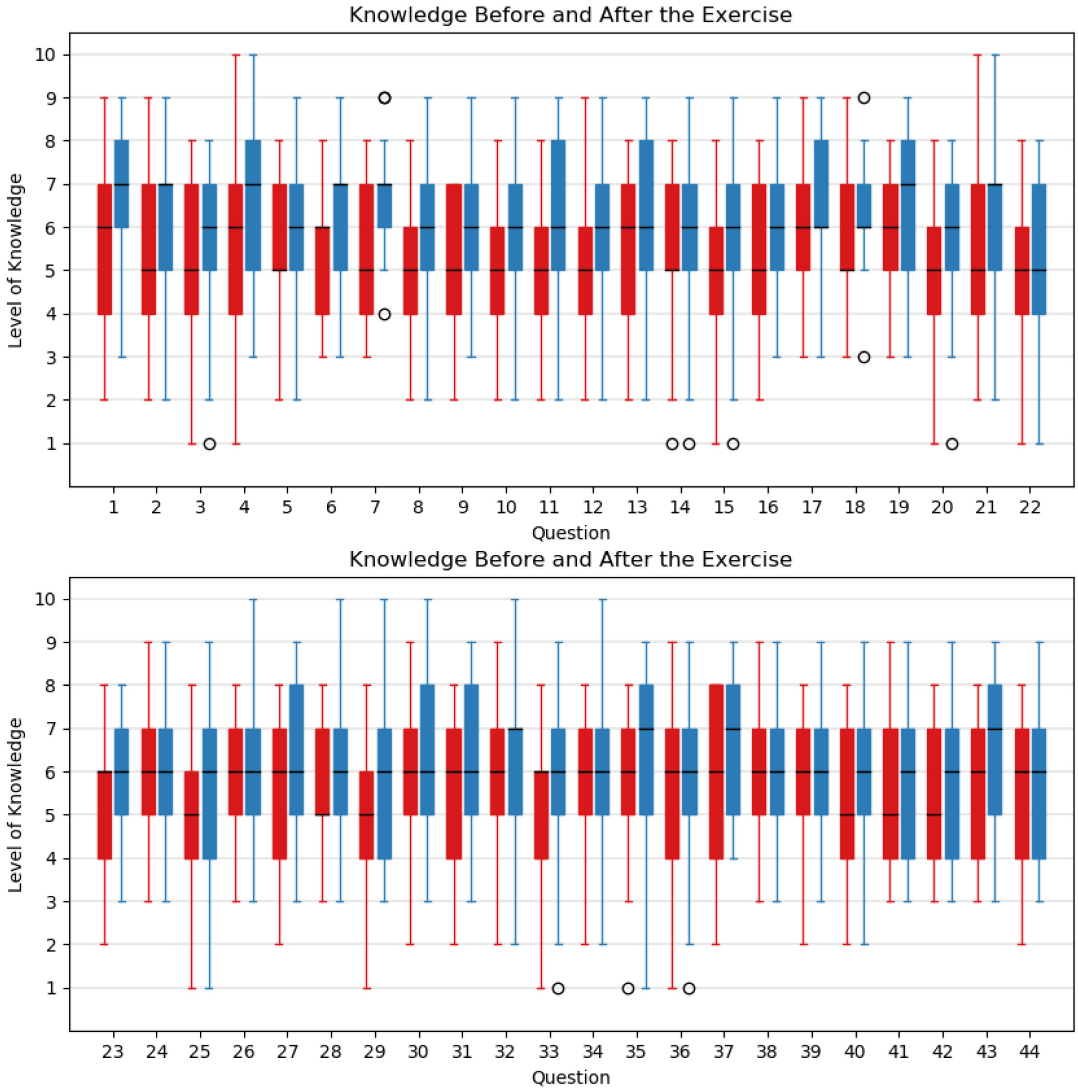


FIGURE 4. Level of knowledge before (red) and after (blue) the exercise in the online exercise

The questionnaire was answered by all 33 students on the course, making it a comprehensive survey of the students in course. Figure 4 shows that statistically significant learning occurred for 43 of the 44 sub-areas of the question set. The only area where, according to the data, no learning took place was 'packet-level analysis using appropriate tools'. Only one of the teams in the exercise used a tool that allowed packet level analysis, thus explaining the phenomenon. The results showed that cybersecurity exercises are an effective pedagogical tool even when organised in an online format. The results strengthened and supported those for the 2019 sample regarding the functionality of cybersecurity training as a pedagogical tool.

Based on the two research samples, it was concluded that cybersecurity exercises, conducted on a comprehensive cyber arena-style training platform, serve as an excellent tool for developing cybersecurity subject-specific competencies. Based on the data, it was evident that, when training platforms are designed according to authentic learning environment theory, the training extensively develops the competencies of students. It is also likely that, when training scenarios on training platforms are realistic (e.g. realistic attack vectors handled with real malware), new skills can easily be developed for working life.

Based on the interviews with lecturing staff, it was evident that the lecturers were pleasantly surprised by the results indicating the students' competency development. They had no previous experience of a cybersecurity exercise conducted entirely using an online training method, and they initially had reservations about the possibility of achieving a successful training outcome. The teachers were particularly concerned that, in an online exercise, communication between students should be facilitated. As a result, the lecturing staff contributed significantly to constructing the communication platform, which was built using the existing Microsoft Teams communication platform due to the tight schedule. The planned and implemented communication platform is shown in Figure 3. Based on their experience, the lecturers identified the transfer of the communication platform to the cyber arena infrastructure as a further development requirement. The transfer was justified on security grounds because using the communication platform for other purposes was likely to interfere with the learning situation. Monitoring individual student performance was found to be significantly challenging and emerged as a developmental issue. Due to the lack of a situational overview, the assessment had to be simplified and performed as a team-level assessment. As a further development, an assessment support tool should be developed to collect statistics on student performance and contribution during the life cycle of the exercise. The data could be utilised as part of the assessment and reflect the performance of a student based on the data produced by the tool.

4.3 Assessment in the cybersecurity exercise (Article V)

The evaluation of cybersecurity education can be approached from several perspectives. Particularly in continuing education, the evaluation of a functional team is often performed as an assessment. In this case, it is based on reflective analysis of the performance of the team involved in the exercise against the set pedagogical goals for the exercise. The evaluation is performed at the team level. This means that the activities of a team member are less important for the evaluation than the activities of the team in its entirety. In evaluation, the different phases of the exercise and the performance of each team are closely analysed. Often, the evaluation results in an analysis of the activities and possibly a list of development points. In practice, evaluation can be performed, for example, according to the categorisation developed by Kirkpatrick, which divides evaluation into the following four levels: (1) reaction, (2) learning, (3) behaviour, and (4) results (Kirkpatrick & Kirkpatrick, 2006).

In a cybersecurity exercise relating to a degree, assessment is usually performed on a student-by-student basis. The reasons for this are the requirement for assessment of parts of the degree course, as well as existing traditions that make student-specific numerical assessment familiar. Brown and Pickford (2006) developed an evaluation model suitable for evaluating an individual in a cybersecurity exercise. It divides the evaluation into the following subsections, the significance and implementation of which must be planned in advance:

Why? The why section answers the questions 'Why is the assessment performed? Why is assessment in the training significant?' In a cybersecurity exercise, an assessment is performed to understand what an individual has achieved. Assessment can also guide the learning goals set for the individual. Assessment aids in motivating individuals to perform the exercise. Assessment can assess the motivation levels of students and their competence and skills, and can provide each student with information about any errors or deficiencies.

What? The what section answers the question 'What is being evaluated?' The cybersecurity exercise assesses the workflow, the performance of individuals, the tasks to be performed by them, and the performance of individuals relating to tasks undertaken as part of a team.

How? The how section explains how assessment is achieved in practice. In the pedagogical model of a cybersecurity exercise shown in Figure 1, situation awareness in practice represents the information collected for evaluation, based on which evaluation is performed. It can be seen from the figure that information for evaluation is collected from several sources throughout the life cycle of an exercise. As part of the assessment, information gathering depends on observations made by a teacher in a classroom. In the studies carried out regarding the online exercise, the need for such a tool emerged as necessary for, in practice, demonstrating the performance of a student during the online exercise.

Who? The who section determines whose duty it is to perform the assessment. Cybersecurity exercises often use different assessments, which are combined to provide a broader and deeper assessment. This involves peer review, which provides insight into the internal work, processes, and performance of a team. The activity and motivation of students to contribute to the exercise at different stages of its life cycle can be assessed by combining peer review with a lecturer's assessment of written reports created by students.

When? The when section determines the timing of the assessment. In a cybersecurity exercise, assessment should be carried out at all stages of its life cycle according to the theory of formative evaluation (Scriven, 1966). The importance of assessment should guide the exercise in practice based on the learning goals set for the activity. Several studies have suggested that the learning outcomes of students improve when assessment is conducted according to formative assessment, which guides learners and assesses their learned skills simultaneously (Leahy & Wiliam, 2012; Thomas et al., 2011).

Formative assessment emphasises the importance of feedback (Hattie, 2003a). Feedback can be divided into three different types: feed-up, feedback, and feed-forward. The feed-up type provides students with information on the set learning goals (i.e. what they should be aiming for). The purpose of the feedback is to continuously refine and specify the set goals. It is also intended to engage and motivate students to carry out learning tasks and thus enable them to achieve the learning objectives. To facilitate exact feedback for students, the learning objectives must be precisely defined. The feed forward type determines the actions required of students. For example, the lecturer can use questions to guide students towards the next stage, enabling the set learning goals to be achieved.

According to Hatti (2003), each feedback type can be used at four different levels:

1. level of tasks: how well the student understands the tasks given to him/her,
2. process level: the process that a student needs to understand what is required of him/her and be able to do it,
3. level of self-direction: feedback guides students to be self-directed and to conduct self-assessment),
4. person level: feedback provides information about the development of the person regarding the set goals.

During cybersecurity exercises, in general, the role of feedback is to guide students towards the learning goals. Because a cybersecurity exercise intentionally simulates a complex operating environment in which students can learn to anticipate difficult-to-predict causal relationships, continuous feedback is important for achieving the objectives of the exercise. In practice, feedback is used to reduce the gap between existing and targeted knowledge.

4.4 Pedagogical requirements for a comprehensive cyber arena (Article IV)

From a traditional perspective, a cybersecurity training platform (cyber range) has been seen narrowly as a particular technology, function, research, or (as in Frank et al., 2017) test environment that uses simulation and a modelled command and control function (Chapman et al., 2017; Frank et al., 2017; Liu et al., 2019; Nagarajan et al., 2012; Subaşu et al., 2017).

In an increasingly complex, networked, digital operating environment, the need to use different cybersecurity training platforms for educational and research applications is continuously increasing. Therefore, as part of the research, a concept was constructed that met the requirements of modern cybersecurity education and enabled learning through cybersecurity practice and the application of learning in a sufficiently realistic teaching environment.

Figure 5 presents a principal description of a research-modelled, modern cybersecurity learning environment called a comprehensive cyber arena. During modelling, special attention was directed to the factors that must be observed to enable the learning environment to correspond to the functionalities of a realistic 2020s operating environment. This was necessary for the set learning objectives to be taught in an environment that simulated with sufficient precision a real operating environment and developed skills that were applicable in a real working environment (Collins & Evans, 2018).

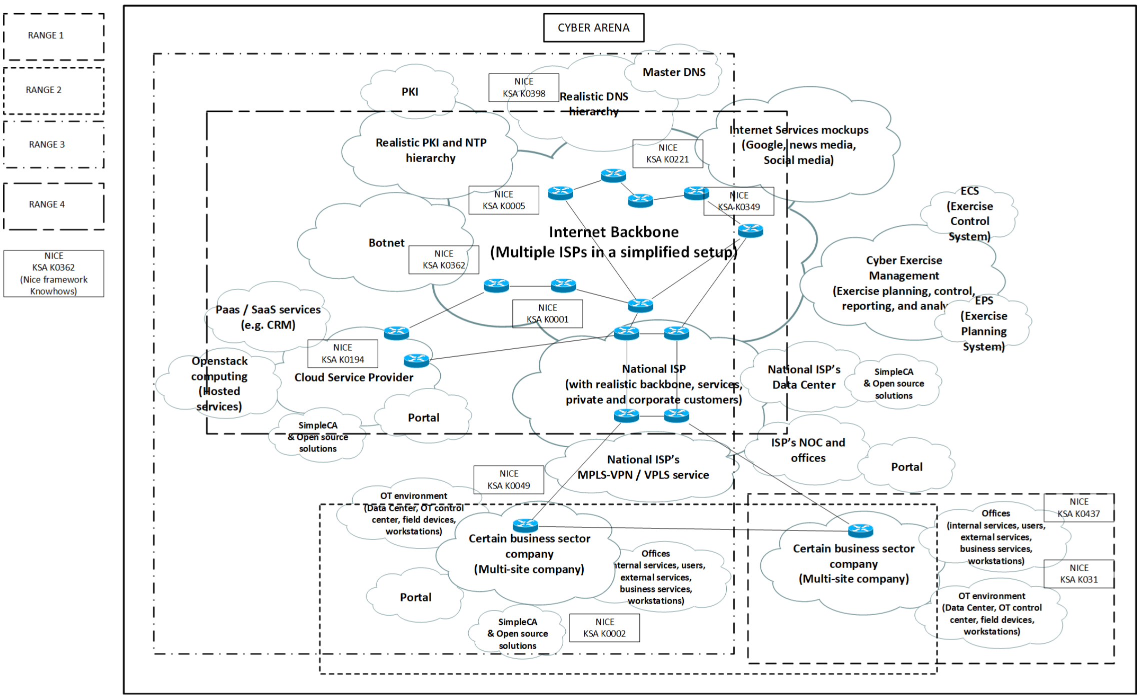

RANGE 1
RANGE 2
RANGE 3
RANGE 4
NICE KSA K0362 (Nice framework Knowhows)
CYBER ARENA
PKI
NICE KSA K0398
Realistic DNS hierarchy
Master DNS
Realistic PKI and NTP hierarchy
NICE KSA K0221
Internet Services mockups (Google, news media, Social media)
NICE KSA K0005
NICE KSA-K0349
ECS (Exercise Control System)
Botnet
NICE KSA K0362
Internet Backbone (Multiple ISPs in a simplified setup)
Cyber Exercise Management (Exercise planning, control, reporting, and analy
EPS (Exercise Planning System)
Paas / SaaS services (e.g. CRM)
NICE KSA K0001
NICE KSA K0194
Openstack computing (Hosted services)
Cloud Service Provider
National ISP (with realistic backbone, services, private and corporate customers)
National ISP's Data Center
SimpleCA & Open source solutions
Portal
SimpleCA & Open source solutions
ISP's NOC and offices
Portal
NICE KSA K0049
National ISP's MPLS-VPN / VPLS service
OT environment (Data Center, OT control center, field devices, workstations)
Certain business sector company (Multi-site company)
Offices (internal services, users, external services, business services, workstations)
Portal
SimpleCA & Open source solutions
NICE KSA K0002
Certain business sector company (Multi-site company)
Offices (internal services, users, external services, business services, workstations)
NICE KSA K0437
NICE KSA K031
OT environment (Data Center, OT control center, field devices, workstations)

FIGURE 5. The model of a comprehensive cyber arena

These requirements must be considered when designing a realistic cyber learning environment (comprehensive cyber arena):

1. realism,
2. isolated and controlled environment,
3. internet simulation,
4. user and network traffic generation,
5. attack execution and simulation.

Realism The overall architecture of a cyber arena should model key internet services, including possible cloud service interfaces and functionality, as well as the information network infrastructure between organisations. Here, the requirements of the authentic learning environment theory are incorporated as a pedagogical principle. Like a real operating environment, the simulated environment must be able to model, to a sufficient degree, the complexity that is present in unpredictable cause-and-effect relationships through the combined effect of technological and functional events.

Isolated and controlled environment A cyber arena must constitute an isolated and controlled environment. It is important to be able to model the behaviour of genuine malware and its traces in the infrastructure in an operating environment, and to be able to do so without any risk of damage to other infrastructure caused by adverse effects, the environment must be isolated from other activities. Environmental security must be monitored and, if necessary, controlled.

User and network traffic generation A cyber arena must be able to simulate the real traffic of telecommunication networks. For centralised control of the operating environment, traffic profiles generated by users, information systems, and various devices must be created in the operating environment. The operating environment thus models the traffic of a real communication environment and creates an opportunity for students to practice detecting threat vectors as they appear in a real operating environment.

Attack execution and simulation A cyber arena must have the ability to perform cyber-attacks and simulate real attack vectors. When attack vectors run as part of legitimate network traffic, functionality corresponding to a realistic operating environment is created for students.

Organisational infrastructure One or more organisational infrastructures must be modelled in a cyber arena environment. Organisational modelling must take sufficient account of the internal processes and functionalities of the organisation, as well as processes connected to other organisations/actors, such as partners, service providers, sub-contractors and customers. When modelling the operations of organisations, it is imperative that both IT and operational technology (OT) functions are taken into consideration.

Collaboration A cyber arena must facilitate the cooperation of those practicing in the operating environment. Collaboration should simulate the functions, requirements, and communication of a real work environment and allow for reflection on one's own work as part of the larger whole. In terms of cybersecurity subject knowledge, individuals acting as part of a team can be taught through a cybersecurity exercise.

Planning, executing, monitoring, and analysing A cyber arena must be able to simulate real-life scenarios. The pedagogical objectives set for the exercise must be considered and monitored at all stages of the life cycle of the exercise. Therefore, separate tools should be used to enable the planning, execution, monitoring, and analysis of the exercise. The tools should allow lecturers to monitor the achievement of set learning goals and, if necessary, guide students towards those goals. The use of the tools should also allow for the assessment of practice and student performance.

4.5 Curriculum development for degree education (Articles VII and VIII)

As the digital operating environment evolves, the requirement for a cybersecurity-focused workforce is constantly growing. According to the annual Cybersecurity Workforce Study published by (ISC)², the required global workforce of cybersecurity professionals is estimated to be over 4 million people (The Annual Cybersecurity Workforce Study published by the ISC²). The existing shortage of skilled cybersecurity personnel was viewed by 60% of respondents as one of the most significant risks in the cybersecurity sector.

Changes in the digital operating environment are rapid. Technologies are updated and renewed continually, and operating environments often combine new technologies with old systems. This creates a great need to maintain an up-to-date curriculum (Ciampa, 2019). To be able to provide training that develops skills in line with the needs of working life, it is essential to pay special attention to curriculum design.

The competence framework and pedagogical methodology were both based on the European Qualifications Framework (EQF) and the European Credit Transfer and Accumulation System (ECTS), according to which the competence levels of the curricula and the dimension scoping of courses are carried out (Council Recommendation of 22 May 2017 on the European Qualifications Framework (EQF) for lifelong learning, 2017; Government Decree on the National Framework for Qualifications and Other Competence Modules, 2017, Finland). Table 2 describes the EQF terminology on which the competency measurement was based.

TABLE 2. EQF terminology

Skills	Means the ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the EQF, skills are described as cognitive (involving the use of logical, intuitive, and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools, and instruments)
Knowledge	Means the outcome of the assimilation of information through learning. Knowledge is the body of facts, principles, theories, and practices that is related to a field of work or study. In the context of the EQF, knowledge is described as theoretical and/or factual
Competence	Means the proven ability to use knowledge, skills, and personal, social, and/or methodological abilities in work or study situations and in professional and personal development

The proposed terminological harmonisation makes it possible to organise multinational training. To integrate the terminology into national training programmes, EU countries are required to adhere to national quality qualifications frameworks (Government Decree on the National Framework for Qualifications and Other Competence Modules. 2017. Finland). Degrees under the EQF framework are defined at eight different levels based on the skills they require (i.e. from EQF level 1 through to EQF level 8).

The ECTS User Guide (Publications Office of the European Union 2015) Provides guidelines for the content of curricula leading to degrees. The aim is to harmonise and standardise the training provided in the European higher education area (The European higher education area in 2020, 2020).

The European Network for Accreditation of Engineering Education defines the competency framework for engineering education. The quality of degree programmes can be verified using the EUR ACE quality classification, which categorises the areas of expertise covered by engineering degrees as follows:

- knowledge and understanding (KU)
- engineering analysis (EA)
- engineering design (ED)
- investigation (IN)
- engineering practice (EP)
- making judgements (MJ)
- communication and teamwork (CT)
- lifelong learning (LL).

The National Initiative for Cybersecurity Education (NICE) published the cybersecurity competency framework for the National Institute of Standards and Technology (NIST). The NICE framework describes cybersecurity work roles and tasks and the competencies associated with them. Competencies are described as knowledge, skills and abilities—abbreviated as KSAs. By aligning KSAs with job roles, training providers can position KSAs in curricula. Figure 6 shows a model that can be used to align the national competencies with degree curricula. The NICE framework describes the precise competency content of each task role and assigns a unique identifier (ID) to each role. The KSAs for the task role can then be included in course descriptions, thus ensuring that the content is consistent with the identified requirements for working life. The process described is a useful and recommended way to ensure and maintain the appropriateness of curricula and their relevance to working life.

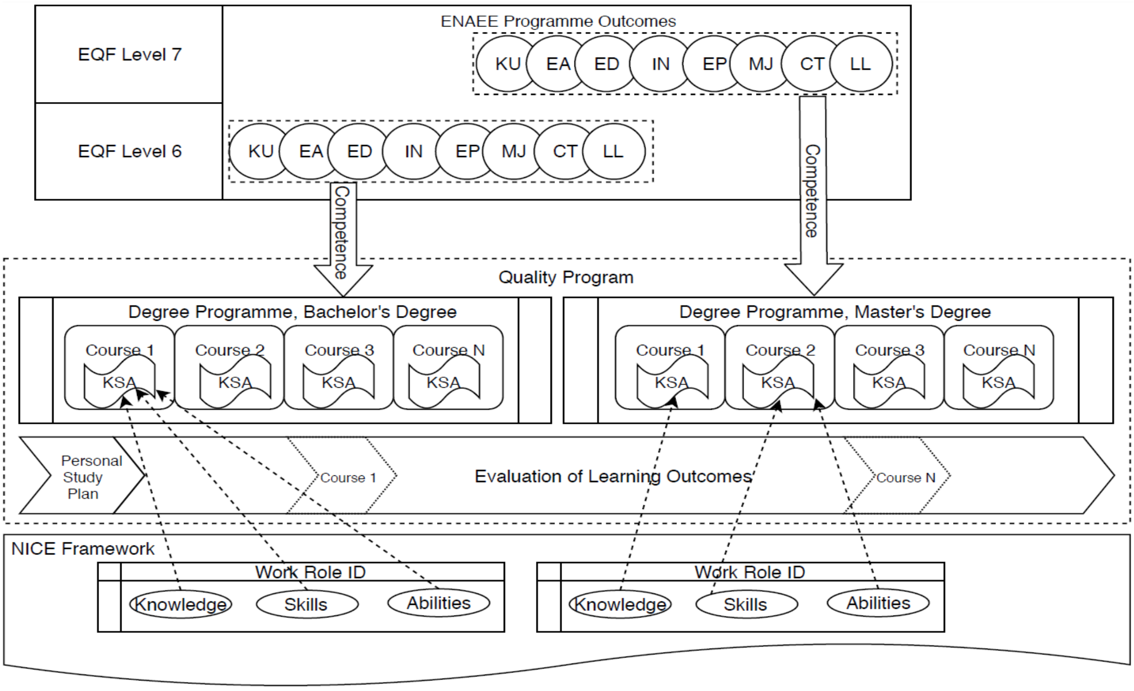


FIGURE 6. Model for a cybersecurity curriculum framework

As stated earlier, the skill requirements for a digitalising world are evolving rapidly. Thus, training providers often find that emerging technologies have evolved to production maturity, but no models like the NIST NICE model have been published for competency criteria. This research developed a curriculum for degree-level education focusing on data analytics and artificial intelligence content, using a theoretical heuristic perimeter model as a model for curriculum development (Dickens, 1977). Figure 7 shows the work process used. The competency base of the curriculum was aligned with fieldwork practice, and the key technologies of data analytics and artificial intelligence were examined using practical laboratory experiments. The resulting knowledge was combined with simultaneous project work, literature analysis, research data, and open data sources. Furthermore, the competence map was supplemented with specific surveys of students' theses. The described method was able to construct the competency profile, curriculum, and course description required by the training provider.

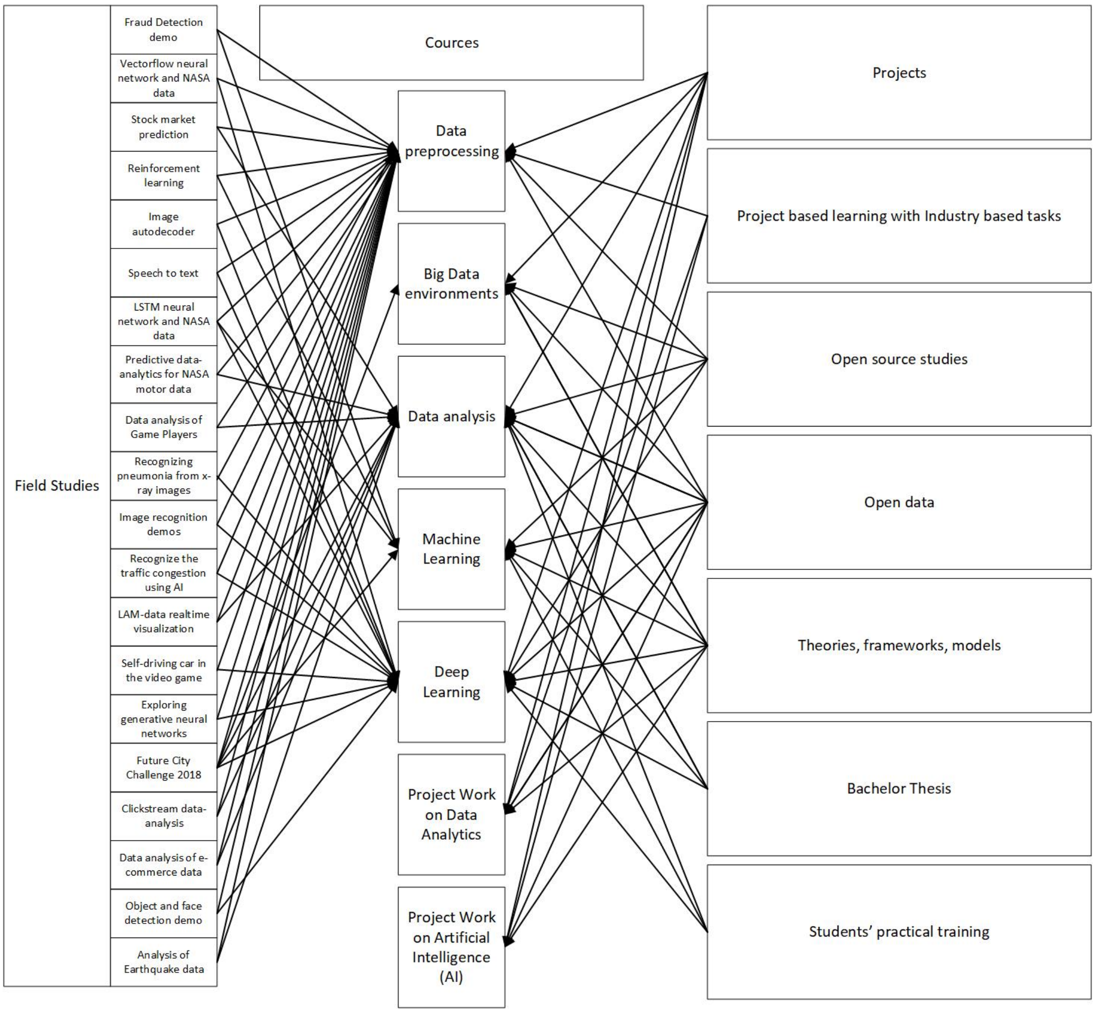

Field Studies
Fraud Detection demo
Vectorflow neural network and NASA data
Stock market prediction
Reinforcement learning
Image autodecoder
Speech to text
LSTM neural network and NASA data
Predictive data-analytics for NASA motor data
Data analysis of Game Players
Recognizing pneumonia from x-ray images
Image recognition demos
Recognize the traffic congestion using AI
LAM-data realtime visualization
Self-driving car in the video game
Exploring generative neural networks
Future City Challenge 2018
Clickstream data-analysis
Data analysis of e-commerce data
Object and face detection demo
Analysis of Earthquake data
Cources
Data preprocessing
Big Data environments
Data analysis
Machine Learning
Deep Learning
Project Work on Data Analytics
Project Work on Artificial Intelligence (AI)
Projects
Project based learning with Industry based tasks
Open source studies
Open data
Theories, frameworks, models
Bachelor Thesis
Students' practical training

FIGURE 7. Heuristic model for curriculum development, case artificial intelligence, and data management

Both of the presented models are useful for curriculum work, especially for maintaining and updating modern ICT curricula. If a widely accepted competency framework is used, the use of the framework is recommended. Synergies were achieved by comparing different national programmes, for example, for students wanting to focus on a specific area of cybersecurity expertise. As the workforce becomes more globally mobile and tasks are increasingly performed independently of physical location, the international comparability of skills and harmonised conception of skills are indisputable advantages.

4.6 Requirements for in-service training (Article IX)

Lifelong learning in technical fields has long been a requirement for maintaining up-to-date knowledge (Steffans, 2015; Van Weert & Kendall, 2006). Those working in the IT sector need to systematically update their skills to stay abreast of technical developments. In in-service cybersecurity training, a commonly used method for updating skills is external course-based training, for which organisations nominate certain individuals (Lindsay et al., 2003). Problems can arise, however, in translating the information learned in the course into organisational competence. In-service cybersecurity exercises are most often conducted by organisations sending functional teams to participate in the exercise, with teams participating in the way they normally would in a real work environment. Usually, two or more organisations participate in the exercise simultaneously.

This approach ensures that genuine interfaces between organisations can be practiced and developed. On a general level, the requirements for cybersecurity exercises organised as in-service training are demanding, and the functionalities modelled in the scenario (i.e. their connections to technical systems within and outside the organisation) are often complex and difficult for the training provider. Orientation must be provided to enable in-service trainees to participate in such exercises, and special attention must be paid not only to training on the functionalities and tools of the teaching environment, but also to the importance of adapting to the exercise. Although the operating environment of the exercise is not likely to be precisely the same as participants' own work environments, the simulated environment can mimic the same phenomena and functions, and the learner can respond with appropriate tools. If the importance of adaptation is not sufficiently clarified during the orientation, considerable time may be taken in the exercise to consider the differences between the tools, with insufficient time being spent on the underlying cybersecurity phenomena.

The research regarding cybersecurity exercises conducted as in-service training relied on Herrington and Oliver's theory of authentic learning environments (Herrington & Oliver, 2000b; Herrington et al., 2014), which has contributed to experiential learning theories (Engstrom, 2001; Kolb et al., 2001). The study included a qualitative interview with five cybersecurity training experts, and the interviews were later subjected to traditional qualitative content analysis (Drisko & Maschi, 2016; Hsieh & Shannon, 2005b). Based on the analysis, using an abductive approach, categories of expertise based on the perspectives of the experts were constructed, as shown in Figure 8 (Graneheim et al., 2017).

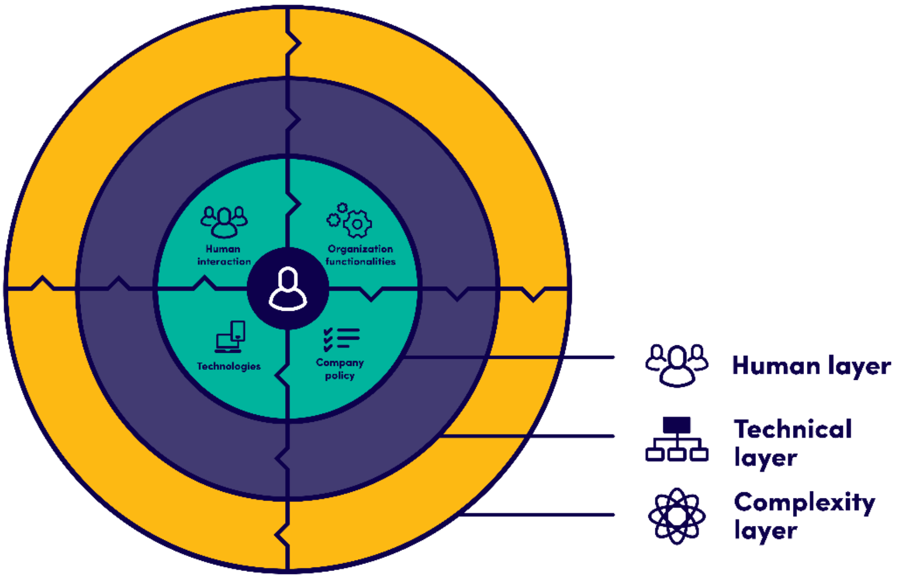


FIGURE 8. Components and categories of optimal in-service cybersecurity training

Based on the interviews, we identified three fundamental components: the *technology layer*, the *human layer*, and the *complexity layer*, which were the three themes that permeated all the categories. The elements of competence in Figure 8 describe the key learning areas of a cybersecurity exercise offered as in-service training. The traditional focus of learning in cybersecurity exercises has been on practicing technical functions. In constructing the categories of competencies based on the interviews, special attention was paid to the fact that a large part of learning relates to areas other than technical matters. Interviewees particularly emphasised practicing appropriate behaviour, interaction, communication, common terminology, and team problem-solving as part of a cybersecurity exercise.

Technologies The technical infrastructure of the cybersecurity operating environment consists of several technical layers, the connections between which in terms of operational processes must be understood and managed. The technical layers can be explained from different perspectives, such as technology-driven or by dividing different technologies into the functionalities to which they relate. In this research, the categorisation was performed so that the technologies and technical functions on the human layer could be influenced by learners through their own activities. These included, for example, the communications infrastructure of the organisation with its servers, infrastructure, and protective technologies such as firewalls. The technical layer surrounding the human layer included technology that the learners could not influence by their own actions, but which affected the actions of learners, such as the internet topology, internet services, and available cloud services.

Organisational functionalities The next human layer block included the organisational functions and functionalities towards which the exercise was targeted. The functionalities or processes that were modelled in the exercise could relate to either the internal functions of the organisation or ones that extended beyond the organisation (e.g. in connection with the activities of a sub-contractor).

Company policies Company policies comprise the rules and general regulations of an organisation relating to its operations and infrastructure maintenance. The guidelines and rules that are created to guide the operations of an organisation should meet operational needs and thus evolve as the operations evolve. However, it often happens that, as activities develop, the instructions for them are not updated synchronously, or vice versa. Therefore, instructions and regulations are a central component of the human layer and were a significant focus of the exercise.

Human interaction This section includes the functionalities mentioned by the interviewed experts (e.g., the importance of communication within the organisation and the importance of practicing it). The activities of an organisation are often divided into several levels and should overlap seamlessly with each other through relevant processes. However, spoken terminology often differs across layers, hindering practical interaction. For cybersecurity training, the interviewees mentioned the importance of practicing and developing spoken terminology and consistent interpretation of organisational processes. This also includes a consistent understanding of operational roles and responsibilities within the organisation.

All the above factors intersect with the technological solutions that define an operating environment and its complexity, which should be simulated as part of an exercise.

5 DISCUSSION

The motivation for the research arose from the authors' work in an organisation that conducts cybersecurity exercises and develops training methodologies and platforms. The author had established that cybersecurity exercises are an excellent tool for competency development, both in education leading to a degree and in in-service training. Feedback from students and organisations participating in the exercises supported the effectiveness of such exercises as a tool for competency development. However, the author observed that there was virtually no research on cybersecurity exercises as a pedagogical tool. Other pedagogical research relating to such exercises was also limited. It was therefore natural to focus the research on the pedagogy of cybersecurity training and thereby address the perceived lack of research.

The aim of the study was to provide a deeper understanding of the pedagogical principles that should be applied to both the construction of training environments and the implementation of exercises. The research questions were:

1. How does a cybersecurity exercise serve as a tool for developing the competencies of individuals?
   a. How can competency development be measured effectively?
   b. How do students develop their knowledge during such exercises?
2. What underlying pedagogical principles should a cybersecurity training platform be based on?
3. How can cybersecurity exercises support lifelong learning:
   a. for curriculum development in education leading to a degree?
   b. for in-service education?

5.1 Pedagogical basis of live cybersecurity exercises

The research achieved the set objectives and answered the research questions. The original research methods were supplemented by an additional methodology as the research process progressed. The quantitative research data revealed students’ competency development during the cybersecurity exercises, in both the on-site and online training. The qualitative research data facilitated a deeper understanding of the requirements for online training and the special features and requirements for in-service training. The qualitative methodology was also adopted to utilise the extensive experience of the researchers and experts involved in the study and to construct a pedagogical model for cybersecurity exercises.

Pedagogical requirements were defined for the learning platform used as the teaching environment for the cybersecurity exercises. Alongside the requirement definition, the term cyber arena was adopted to express the difference between a comprehensive cyber arena and standard cyber range-style learning environments built according to several requirements and approaches. Using a cyber arena-style learning environment enables teaching to be carried out in a realistic operating environment that supports the practicing of complex problem-solving skills. The use of a cyber arena style teaching environment also meets the educational needs of in-service training on modern emerging technologies.

The study also identified the pedagogical theories that should be applied to the design, implementation, and evaluation of cybersecurity exercises and determined the pedagogical factors relating to such an education event. The study developed a cybersecurity exercise assessment model that tied pedagogic principles to the exercise life cycle and determined the assessment based on an individual learning framework.

Regarding the quantitative data, two research samples provided evidence that students experienced a significant increase in their cybersecurity knowledge through the exercises. The previously mentioned NICE NIST framework, selected as the basis for the questionnaire, proved to be useful, although it posed challenges for determining the appropriate scope of the question battery. The 44-question survey that was distributed to students extensively measured their cybersecurity competencies and provided information on the function of exercises as a pedagogical tool. In future research, the questionnaire should focus in detail on specific cybersecurity phenomena, which would shorten the set of questions and reduce the workload for respondents. If there is a need to measure generic cybersecurity expertise and its development on a large scale, the questions should be condensed into broader categories to achieve a more reasonable number of questions. The 1–10 scale for the questions was justified and functional, providing accurate information about changes in competencies. In the future, however, descriptors should be provided to assist the respondents in assessing their own competencies on the given scale. Numerical competency assessments could be aligned with curriculum competency assessments. The amount of quantitatively measurable data was small despite using two samples. In the second sample, all the students who participated in the exercise answered the questionnaire, which contributed to eliminating the large loss of responses that was problematic in the first sample. The statistical analysis was relatively narrow because it was performed on a numerically small sample and did not provide accurate information about the phenomena under study. However, the samples taken together provided a generalisable overview of learning during a cybersecurity exercise.

The methods employed to organise the cybersecurity exercises differed from each other. Due to the unavoidable circumstances at the time, the second exercise had to be converted into an online exercise, which provided an opportunity to study an online exercise and its functionality as a competence developer. The result was a pleasant surprise for the lecturing staff and researchers, which resulted in increased confidence to further develop online exercise methods and practices. The exercises utilised the same cybersecurity training platform, so the samples and their results supported each other. Based on the results, it was evident that cybersecurity exercises are an excellent tool for competency development.

The study determined the specific features required for undergraduate higher education and in-service training. Education leading to a degree is guided in practice by the curriculum. The study presented two different methods for developing and maintaining a curriculum that meets the needs of working life in terms of content. Cybersecurity exercises could be included as part of the curriculum and used to provide students with an opportunity to use and apply the knowledge they have acquired during the degree programme. A special feature of online training is a training platform tailored to the needs of the customer, in which (additional to the technological infrastructure) the functionalities and processes of the organisation to which the technology is related are modelled. Also, the modelling of the remaining ecosystem associated with the organisation and its operations should be designed with adequate accuracy and scope.

5.2 Trustworthiness of the research

When mixed methods are used for research, the researcher must ensure that the qualitative and quantitative research methods complement each other (Johnson, 2007). Certain methods for ensuring the validity and reliability of quantitative research are widely used and accepted, but the methodology used in qualitative research differs (Golafshani, 2003). In this section, I address the trustworthiness of the research based on the criteria of (1) credibility, (2) transferability, (3) dependability, and (4) confirmability (Lincoln, 1985).

Credibility can be understood as a measure of the truthfulness of research findings (Lincoln, 1985; Tashakkori et al., 2020; Tashakkori et al., 1998). To evaluate the credibility of this research, the following functions were considered. The research design was described in the papers as accurately as possible. The various stages of the research process and the related methodology were also described in detail in the papers. In the interview coding phase, the researchers conducted the work independently and thereafter came together to reflect on the work done, thus ensuring the coherence and contribution of the coding work.

The size of the sample for the quantitative analysis of students' experienced learning presented in Articles III and VI remained small. Considering that the exercises were slightly different (on-site/online) and both samples showed that the students experienced statistically significant learning, it can be confidently stated that the findings for the two samples supported each other. In the aggregation phase of the study, qualitative and quantitative data were used to support each other and to add value to the study findings.

Transferability describes the transferability or applicability of research findings to another context or situation (Lincoln, 1985; Tashakkori et al., 2020; Tashakkori et al., 1998). Making extensive generalisations of the findings would require a broader sample than the one used in this study. The group of students who participated in the study differed in their backgrounds in terms of age, gender, possible previous experience, and national characteristics. However, the sample represented the profile of an undergraduate cybersecurity student. Further research could determine the possible effects of background variables. The descriptions of the steps of the research process provided in the papers should help to assess the generalisability of the research results and enable the findings to be used in other contexts.

Dependability is a similar evaluation criterion to reliability in the tradition of quantitative research (Tashakkori et al., 1998). Reliability can be understood as processes aiming to ensure that the research results remain the same if the research is repeated in the same frame of reference (Guba & Lincoln, 1994). When assessing dependability in the context of qualitative research, it is important to establish a systematic, logical, and scientific coding scheme (Folger et al., 1984) . In this study, we used the coding method established by Hsieh and Shannon (2005). In the papers for which we used conventional content analysis, the researchers collaborated extensively to ensure consistent categorisation and coding (Elliott, 2018). For the quantitative research papers, the aim was to use a solid methodology for the research design and the data collection process and thus ensure the dependability of the research results. Similar ways of working were also used for the analysis, with all the researchers contributing to the analysis. We also used different tools like Python programming, Microsoft Excel, and SPSS Statistics to confirm the results of the quantitative analyses.

Confirmability refers to scientific objectivity that seeks to eliminate potential errors in results due to the skill deficiencies or preconceptions of researchers (Shenton, 2004). To ensure confirmability, mixed methods were chosen as the research methodology. However, it should be noted that while the methodology helped to ensure the confirmability of the study, the possibility of bias could not be completely eliminated since the instruments for study were designed by the researchers (Miles & Huberman, 1984; Patton, 2002). These arguments were included in the research papers, and potential researcher bias was recognised.

5.3 Further research

In further research, it would be advisable to increase the size of the research sample to evaluate students’ competency development during cyber exercises more thoroughly. A higher number of responses would enable researchers to analyse possible differences in the respondents’ backgrounds and the implemented teaching methods, which could be studied in relation to changes in the digital operating environment.

Research should also be extended to cybersecurity exercises intended to facilitate the development of organisational competencies. It should be noted that when cybersecurity exercises are offered as in-service training, they differ from the traditional model for in-service training. In in-service training, an organisation often sends representatives of an existing team or function to attend cybersecurity exercises. How the simultaneous training of teams contributes to the integration of newly learned competencies into the knowledge capital of an organisation would be an interesting topic for organisational research.

The cyber arena concept presented in this study should be further tested in subsequent studies, especially regarding the definition of technical requirements.

YHTEENVETO (SUMMARY IN FINNISH)

Digitalisoituvassa maailmassa työ ja sen tekemisen tavat muuttuvat nopeudella, jota ei liene aiemmin ole nähty. Digitalisaatio tuo mukanaan uusia tapoja toimia niin työelämässä kuin vapaa-ajallakin. Suhteessa kehittyvään teknologiaan ihminen itsessään muuttuu melko hitaasti. Pohdittaessa ihmisen kykyä adaptoitua muutokseen keskeinen huomio tulisi kohdistaa ihmisen tapaan oppia. Oppimisen teoriat ovat jo vuosisatoja muodostaneet kunkin ajan mukaisen käsityksen oppimisen prosessista ja siihen liittyvistä ihmisen kognitiivisista prosesseista. Tämän vuoksi erityistä huomiota tulisi kiinnittää digitalisaation mukanaan tuomiin uusiin osaamisvaatimuksiin sekä tapoihin opettaa.

Covid-19-pandemia pakotti opetuksen kaikilla koulutuksen tasoilla etäopetusmoodiin. Kun epidemiaa ja poikkeuksellisia opetusjärjestelyjä on kestänyt noin vuoden ajan, olemme jo huomanneet, että etäopetus ei sovellu kaikille oppijoille. Etäopetus vaatii oppijoilta poikkeuksellisen kypsää itseohjautuvuutta ja kykyä itsenäiseen ongelmanratkaisuun. Kun opetuksen parhaita käytäntöjä koronan jälkeisen ajan toimintaympäristössä pohditaan, tulee erityistä huomiota kiinnittää ihmisten välisen vuorovaikutuksen mahdollistamiseen niin digitaalisessa kuin fyysisessäkin opetusympäristössä. Ihminen tarvitsee vuorovaikutusta, joka käytännössä on opettajien ohjausta, vertaisten kanssa tehtävää yhteistyötä ja yhdessä oppimista. Näiden elementtien mahdollistaminen etäopetuksessa, joka käytännössä toteutetaan digitaalisessa toimintaympäristössä, tarvitsee huomiota ja kehittämistoimia. Edellä mainitut ilmiöt ja vaatimukset ovat löydettävissä vaatimuksina myös kyberturvallisuuden koulutuksessa.

Kyberturvallisuuden toimintaympäristö on erittäin laaja-alainen ja sen voidaan katsoa sisältävän useita erilaisia ammatillisia työnkuvia. Laaja-alaisuuden lisäksi kybertoimintaympäristöä ilmentää tietty kompleksisuus, joka muodostuu erilaisista teknologisista toimintaympäristöistä, joihin liittyy fyysisisä toimintoja sekä prosesseja, joiden toiminnot ilmentyvät sekä digitaalisesti että fyysisesti. Lisäksi toimintaan ja sen järjestäytymiseen vaikuttaa inhimillinen vektori, jossa käyttäjän tai muuten toimintaan osallisena olevan henkilön toiminnalla on suuri vaikutus toiminnon käytännön toteumaan. Jotta kokonaisuus voitaisiin hallita ja ymmärtää, tulisi opetuksessa kyetä ilmentämään mainittu kompleksisuuden ulottuvuus. Näin opiskelijalla on mahdollisuus kasvattaa osaamista ja kykyä ennakoida syy-seuraussuhteita. Kyberturvallisuusharjoittelu on vakiinnuttanut paikkansa osana kyberturvallisuuden koulutusta. Harjoitukset toimivat hyvänä opetusmetodina erityisesti sellaisille oppijoille, joilla osaaminen on jo hyvällä tasolla. Tutkimuksessa määritetty Cyber Arena -tyylinen harjoitusympäristö mahdollistaa toiminnan harjoittelun osana tiimiä ja kompleksisten syy-seuraussuhteiden harjoituttamisen realistisessa oppimisympäristössä, joka tukee opitun osaamisen siirtämistä työelämään.

Tässä tutkimuksessa on määritetty kyberturvallisuusharjoittelun pedagogista teoriaa ja määritellyn teoreettisen viitekehyksen vaatimuksia opetusympäristölle. Useiden vuosien aikana toimeenpannut kyberturvallisuusharjoitukset olivat osoittaneet, että käytännössä harjoitus toimii erinomaisena osaamisen kehittämisen välineenä. Tutkimuksellista dataa osaamisen kehittymisestä kyberturvallisuusharjoituksessa ei kuitenkaan ole ollut saatavilla. Tämä tutkimus on osaltaan täyttänyt tuota tutkimuksellisen tiedon vajetta. Tässä tutkimuksessa on määritetty kysymyspatteristo käyttäen hyväksi yleisesti käytettyä NIST NICE -kehystä, jolla voidaan mitata kyberturvallisuusharjoituksessa tapahtuvaa oppimista.

Tutkimuksen tulosten perusteella voidaan sanoa, että kyberturvallisuusharjoitus toimii erinomaisena opetusympäristönä ja opetusmetodina. Osana tutkimusta kartoitettiin myös elinikäisen oppimisen näkökulmasta täydennyskoulutuksen tarpeita ja erityisiä näkökulmia kyberturvallisuusharjoittelussa. Tulosten perusteella kyberturvallisuusharjoitus soveltuu myös täydennyskoulutukseen, ja tällöin harjoituksessa tulisi huomioida myös ns. ei tekniset kyberturvallisuuden osa-alueet kuten tiimimäinen toiminta, vuorovaikutus, käytetty organisaation yhteinen terminologia, organisaation sisäiset ja ulkoiset prosessit, haavoittuvuusanalyysi, riskienhallinta ja päätöksenteko. Näin toimien kyberturvallisuusharjoituksella voidaan kehittää organisaation osaamista useilla eri alueilla ja tasoilla.

REFERENCES

The European higher education area in 2020. (2020). Luxembourg: Publications Office.

Abdulwahed, M., & Nagy, Z. K. (2011). The TriLab: A novel ICT based triple access mode laboratory education model. *Computers & Education 56*(1), 262–274.

Angafor, G. N., Yevseyeva, I., & He, Y. (2020). *Bridging the Cyber Security Skills Gap: Using Tabletop Exercises to Solve the CSSG Crisis*. Joint International Conference on Serious Games. Springer, 117–131.

Bariran, S., Sahari, K., & Yunus, B. (2013). 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.

Brown, S., & Pickford, R. (2006). *Assessing skills and practice*. Routledge.

Carayannis, E. G., Campbell, D. F., & Efthymiopoulos, M. P. (2018). *Handbook of cyber-development, cyber-democracy, and cyber-defense.* Springer.

Chapman, S., Smith, R., Maglaras, L., & Janicke, H. (2017). Can a network attack be simulated in an emulated environment for network security training? *Journal of Sensor and Actuator Networks* 6, 16. Vol.6, Iss.3.

Chen, Z., Yan, L., He, Y., Bai, D., Liu, X., et al. (2018). *Reflections on the Construction of Cyber Security Range in Power Information System*. 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2093–2097.

Chou, P. & Feng, S. (2019). Using a tablet computer application to advance high school students' laboratory learning experiences: A focus on electrical engineering education. *Sustainability 11*(2), 381.

Ciampa, M. (2019). Do students and instructors see cybersecurity the same? A comparison of perceptions about selected cybersecurity topics. *International Journal for Innovation Education and Research 7*(1), 121–135.

Clark, V. L. P., Creswell, J. W., Green, D. O., & Shope, R. J. (2008). *Mixing Quantitative and Qualitative Approaches: Handbook of Emergent Methods* p. 363. The Guilford Press.

Collins, H. & Evans, R. (2018). A sociological/philosophical perspective on expertise: The acquisition of expertise through socialization. In K. A. Ericsson, R. R. Hoffman, A. Kozbelt, & A. M. Williams (Eds.) *The Cambridge Handbook of Expertise and Expert Performance.* (2nd edition) Cambridge University Press, pp. 21–32.

Committee, Secretariat of the Security (2019). Finland's Cyber Security Strategy, Government Resolution 3.10.2019.

Committee, Secretariat of the Security (2013). Finland's Cyber Security Strategy, Government Resolution 24.1.2013.

Council Recommendation of 22 May 2017 on *the European Qualifications Framework for Lifelong Learning* (EQF). Available at: https://www.cedefop.europa.eu/fi/events-and-projects/projects/european-qualifications-framework-eqf. Accessed: 05.01.2021.

Dausey, D. J., Buehler, J. W., & Lurie, N. (2007). Designing and conducting tabletop exercises to assess public health preparedness for manmade and naturally occurring biological threats. *BMC Public Health 7*(1), 1–9.

Davis, J. & Magrath, S. (2013). A survey of cyber ranges and testbeds. *No.* DSTO-GD-0771. Defence Science and Technology Organization Edinburgh (Australia) Cyber and Electronic Warfare Div.

Dawson, J. & Thomson, R. (2018). The future cybersecurity workforce: Going beyond technical skills for successful cyber performance. *Frontiers in Psychology* 9, 744. Vol. 9.

Debatty, T., & Mees, W. (2019). *Building a Cyber Range for Training Cyberdefense Situation Awareness*. 2019 International Conference on Military Communications and Information Systems (ICMCIS), 1–6. IEEE.

Deckard, G. M. (2018). *Cybertropolis: Breaking the Paradigm of Cyber-Ranges and Testbeds*. 2018 IEEE International Symposium on Technologies for Homeland Security (HST), 1–4. IEEE.

Dhawan, S. M., Gupta, B. M., & Elango, B. (2020). *Global Cyber Security Research Output (1998–2019): A Scientometric Analysis*. Science & Technology Libraries, pp. 1–18.

Dickens, D. (1977). *Hermeneutics and Ethnomethodology.* Southwestern Sociological Association.

Dinevski, D., & Kokol, P. (2004). ICT and lifelong learning. *European Journal of Open, Distance and E-Learning 7*(2).

Dodig-Crnkovic, G. (2010). Constructive research and info-computational knowledge generation. In 359–380. Springer, Berlin, Heidelberg.

Doupé, A., Egele, M., Caillat, B., Stringhini, G., Yakin, G., et al. (2011). *Hit 'em where it Hurts: A Live Security Exercise on Cyber Situational Awareness.* Proceedings of the 27th Annual Computer Security Applications Conferenc*e*, 51–61. Association for Computing Machinery.

Drisko, J. W., & Maschi, T. (2016). Content analysis. *Pocket Guides to Social Work R*. Oxford University Press.

Efland, A. D. (1995). The spiral and the lattice: Changes in cognitive learning theory with implications for art education. *Studies in Art Education 36*(3), 134–153.

Elliott, V. (2018). Thinking about the coding process in qualitative data analysis. T*he Qualitative Report 23*(11), 2850–2861.

Emin-Martinez, V., & Ney, M. (2013). Supporting teachers in the process of adoption of game based learning pedagogy. In P. Escudeiro & C. Vaz de Carvalho (Eds.) *ECGBL 2013 - European Conference on Games Based Learning. Porto, Portugal*: (ACPI), pp. 156–162.

Engeström, Y. (2001). Expansive learning at work: Toward an activity theoretical reconceptualization. *Journal of Education and Work 14*(1), 133–156.

Ericsson, A. K. (2008). Deliberate practice and acquisition of expert performance: A general overview. *Academic Emergency Medicine 15*(11), 988–994

Ernits, M., Maennel, K., Mäses, S., Lepik, T., & Maennel, O. (2020). *From Simple Scoring towards a Meaningful Interpretation of Learning in Cybersecurity Exercises*. ICCWS 2020 15th International Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited, p. 135.

European Defence Agency, EDA, "Cyber ranges federation project reaches new milestone," https://www.eda.europa.eu/info- hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation- project-reaches-new-milestone, Sept 2018, Accessed: 13 January 2020.

Ferguson, B., Tall, A., & Olsen, D. (2014). *National Cyber Range Overview*. 2014 IEEE Military Communications Conference, pp. 123–128.

Folger, J. P., Hewes, D. E., & Poole, M. S. (1984). Coding social interaction. In *Progress in the Communication Sciences*. Ablex.

Frank, M., Leitner, M., & Pahi, T. (2017). Design Considerations for Cyber Security Testbeds: A Case Study on a Cyber Security Testbed for Education. 2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing, 15th International Conference on Pervasive Intelligence and Computing, 3rd International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), pp. 38–46.

Geers, K. (2010). Live fire exercise: preparing for cyber war. *Journal of Homeland Security and Emergency Management 7*(1). Vol 7., issue 1. article 74.

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report, 8*(4), 597–607.

Government Decree on the National Framework for Qualifications and Other Competence Modules. (2017). Finland National Qualifications Frameworks (NQFs). Available at: https://www.oph.fi/en/education-and-qualifications/qualifications-frameworks

Graneheim, U. H., Lindgren, B., & Lundman, B. (2017). Methodological challenges in qualitative content analysis: A discussion paper. *Nurse Education Today* 56, 29–34. Vol 56.

Guba, E. G., & Lincoln, Y. S. (1994). Competing paradigms in qualitative research. *Handbook of Qualitative Research 2* (105, 163–194).

Hattie, J. (2003). *Teachers Make a Difference, What is the Research Evidence? Australian Council for Educational Research (ACER)*

He, Y., Yan, L., Liu, J., Bai, D., Chen, Z., et al. (2019). Design of Information System Cyber Security Range Test System for Power Industry. *2019 IEEE Innovative Smart Grid Technologies – Asia* (ISGT), pp. 1024–1028. IEEE.

Herrington, J. (2006). *Authentic E-Learning in Higher Education: Design Principles for Authentic Learning Environments and Tasks*. E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education. pp. 3164–3173. Association for the Advancement of Computing in Education (AACE).

Herrington, J. & Oliver, R. (2000). An instructional design framework for authentic learning environments. *Educational Technology Research and Development 48*(3), 23–48.

Herrington, J., Reeves, T. C., & Oliver, R. (2014). Authentic learning environments. In *Handbook of Research on Educational Communications and Technology*. Springer, pp. 401–412.

Hirsjärvi, S., & Hurme, H. (2008). *Tutkimushaastattelu: teemahaastattelun teoria ja käytäntö*. Helsinki: Gaudeamus Helsinki University Press.

Hoffman, L. J., Rosenberg, T., Dodge, R., & Ragsdale, D. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy 3*(5), 27–33.

Hsieh, H., & Shannon, S. E. (2005). Three approaches to qualitative content analysis. *Qualitative Health Research 15*(9), 1277–1288.

Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber security threats and vulnerabilities: a systematic mapping study. *Arabian Journal for Science and Engineering 45*(4), 3171–3189.

Hurmerinta-Peltomäki, L., & Nummela, N. (2006). Mixed methods in international business research: A value-added perspective. *Management International Review 46*(4), 439–459.

ISC (2019) *Cybersecurity Workforce Study – ISC2*. Available at: https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=1827084508A24DD75C60655E243EAC59ECDD4482. Accessed: 05.01.2021.

Jin, G. (2018). *Game-Based Cybersecurity Training for High School Students*. In SIGCSE '18: Proceedings of the 49th ACM Technical Symposium on Computer Science Education. ACM, pp. 68–73.

Johnson, R. (2007). Toward a definition of mixed methods research. *Journal of Mixed Methods Research 1*(2), 112–133.

Johnson, R. B. & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher 33*(7), 14–26.

Jones, K. (2018). The core cyber-defense knowledge, skills, and abilities that cybersecurity students should learn in school: Results from interviews with cybersecurity professionals. *ACM Transactions on Computing Education* (TOCE) *18*(3), 1–12.

Kalaniti, K., & Campbell, D. M. (2015). Simulation-based medical education: Time for a pedagogical shift. *Indian Pediatrics 52*(1), 41–45.

Kasanen, E. (1993). The constructive approach in management accounting research. *Journal of Management Accounting Research* 5, 243.

Kazemi, N. (2010). IPsecLite: a tool for teaching security concepts.

Keating, P. J. (1995). A framework for classifying and evaluating the theoretical contributions of case research in management accounting. *Journal of Management Accounting Research 7*, 66.

Kick, J. (2014). *Cyber Exercise Playbook*. MITRE Corp., Bedford, MA.

Kim, J., Maeng, Y., & Jang, M. (2019). Becoming invisible hands of national live-fire attack-defense cyber exercise. *2019 IEEE European Symposium on Security and Privacy Workshops* (EuroS&PW). IEEE, pp. 77–84.

Kirkpatrick, D. L., & Kirkpatrick, J. D. (2006). *Evaluating Training Programs.* Berrett-Koehler Publishers, Inc.

Knowles, M. S. (1995). *Designs for adult learning: Practical resources, exercises and course outlines from the father of adult learning.* American Society for Training & Development.

Kolb, D. A., Boyatzis, R. E. & Mainemelis, C. et al. (2001). Experiential learning theory: Previous research and new directions. *Perspectives on Thinking, Learning, and Cognitive Styles 1*(8), 227–247.

Laal, M. (2013). Collaborative learning; Elements. *Procedia Social and Behavioral Sciences 83*, 814–818.

Lal, S., Lucey, A. D., Lindsay, E. D., Treagust, D. F., Mocerino, M., et al. (2020). Perceptions of the relative importance of student interactions for the attainment of engineering laboratory-learning outcomes. *Australasian Journal of Engineering Education*, 1–10.

Leahy, S., & Wiliam, D. (2012). From teachers to schools: Scaling up professional development for formative assessment. *Assessment and Learning* 2, 49–71.

Lehtiranta, L., Junnonen, J., Kärnä, S., & Pekuri, L. (2016). The constructive research approach: Problem solving for complex projects. *Designs, Methods and Practices for Research of Project Management*. Gower.

Lehto, M. (2020). *Cyber Security Capacity Building: Cyber Security Education in Finnish Universities.*

Libicki, M. C. (2007). *Conquest in Cyberspace: National Security and Information Warfare.*

Lincoln, Y. S. (1985). Guba. EG (1985). *Naturalistic Inquiry*. Sage.

Lindsay, A., Downs, D., & Lunn, K. (2003). Business processes—attempts to find a definition. *Information and Software Technology 45*(15), 1015–1019.

Linn, Y. (2011). An ultra-low cost wireless communications laboratory for education and research. *IEEE Transactions on Education 55*(2), 169–179.

Liu, H., Han, W., & Jia, Y. (2019). *Construction of Cyber Range Network Security Indication System Based on Deep Learning*. 2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC), 495–502.

Luiijf, E. (2012). *Understanding Cyber Threats and Vulnerabilities: Critical Infrastructure Protection*, 52–67.

Lukka, K. (2000). The key issues of applying the constructive approach to field research. In: Reponen, T., Ed., Management Expertise in the New Millennium: In Commemoration of the 50th Anniversary of Turku School of Economics and Business Administration. University of Turku, pp. 113-128.

Lukka, K., & Tuomela, T. (1998). *Testattuja ratkaisuja liikkeenjohdollisiin ongelmiin: konstruktiivinen tutkimusote. Yritystalous* 4(98), 23–29.

Martyn, S. 2008. *Quantitative Research Design*. Retrieved July 8, 2011.

Mäses, S., Kikerpill, K., Jüristo, K., & Maennel, O. (2019). *Mixed Methods Research Approach and Experimental Procedure for Measuring Human Factors in*

Cybersecurity Using Phishing Simulations. 18th European Conference on Research Methodology for Business and Management Studies, 218.

Merriam, S. B. (2004). The role of cognitive development in Mezirow's transformational learning theory. *Adult Education Quarterly 55*(1), 60–68.

Merriam, S. B. & Bierema, L. L. (2013). *Adult Learning: Linking Theory and Practice*. John Wiley & Sons.

Miles, M. B. & Huberman, A. M. (1984). Qualitative data analysis: A sourcebook of new methods. In *Qualitative Data Analysis: A Sourcebook of New Methods*, p. 263.

Miller, G. E. 1990. The assessment of clinical skills/competence/performance. *Academic Medicine 65*(9), 63.

Molina-Azorin, J. F. (2012). Mixed methods research in strategic management: Impact and applications. *Organizational Research Methods 15*(1), 33–56.

Moser, A. & Cohen, M. I. (2013). Hunting in the enterprise: Forensic triage and incident response. *Digital Investigation 10*(2), 89–98.

Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012). *Exploring Game Design for Cybersecurity Training*. 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), pp. 256–262.

Nevavuori, P. & Kokkonen, T. (2019). Requirements for Training and Evaluation Dataset of Network and Host Intrusion Detection System. In Rocha, H. Adeli, L. P. Reis, S. Costanzo & ra (Eds.) *New Knowledge in Information Systems and Technologies*. Springer International Publishing, pp. 534-546.

Nevgi, A. & Lindblom-Ylänne, S. (2003). *Oppimisnäkemykset antavat perustan opetukselle. In Yliopisto-ja korkeakouluopettajan käsikirja*. WSOY, pp. 82–116.

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. National Institute of Standards and Technology.

NIST, (2017) *National Institute of Standards and Technology National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. 2017.* Available at: DOI=https://doi.org/10.6028/NIST.SP.800-181.

Nordio, M., Mitin, R., & Meyer, B. (2010). *Advanced Hands-On Training for Distributed and Outsourced Software Engineering*. Proceedings of the 32nd ACM/IEEE International Conference on Software Engineering, Volume 1, pp. 555-558.

Norris, N. (1997). Error, bias and validity in qualitative research. *Educational Action Research 5*(1), 172–176.

Nyre-Yu, M. (2021). *Identifying Expertise Gaps in Cyber Incident Response: Cyber Defender Needs vs. Technological Development*. Proceedings of the 54th Hawaii International Conference on System Sciences, 1978.

Nyström, S., Dahlberg, J., Edelbring, S., Hult, H., & Abrandt Dahlgren, M. (2016). Debriefing practices in interprofessional simulation with students: A sociomaterial perspective. *BMC Medical Education* 16 (1).

Panitz, T. (1999). *Collaborative versus Cooperative Learning: A Comparison of the Two Concepts Which Will Help Us Understand the Underlying Nature of Interactive Learning*. ERIC Institute of Education Sciences.

Park, Y. S., Choi, C. S., Jang, C., Shin, D. G., Cho, G. C., et al. (2019). *Development of Incident Response Tool for Cyber Security Training Based on Virtualization and Cloud*. 2019 International Workshop on Big Data and Information Security (IWBIS). IEEE, pp. 115–118.

Parrish, A. (2018). Global perspectives on cybersecurity education for 2030: A case for a meta-discipline.

Patton, M. Q. (2002). Two decades of developments in qualitative inquiry: A personal, experiential perspective. *Qualitative Social Work 1*(3), 261–283.

Pham, C., Tang, D., Chinen, K., & Beuran, R. (2016). CyRIS: *A Cyber Range Instantiation System for Facilitating Security Training*. Proceedings of the Seventh Symposium on Information and Communication Technology, pp. 251–258.

Pöyhönen, J. & Lehto, M. (2020). *Cyber Security: Trust Based Architecture in the Management of an Organization's Security*. ECCWS 2020 20th European Conference on Cyber Warfare and Security. Academic Conferences and Publishing Limited, p. 304.

Pridmore, L., Lardieri, P., & Hollister, R. (2010). *National Cyber Range (NCR) Automated Test Tools: Implications and Application to Network-Centric Support Tools*. 2010 IEEE AUTOTESTCON, pp. 1–4.

Publications Office of the European Union (2015). *ECTS Users' Guide*.

Rauste von Wright, M. & von Wright, J. (1996). Oppiminen ja koulutus. Aikuiskasvatus *16*(1), 50–52.

Rege, A., Obradovic, Z., Asadi, N., Parker, E., Masceri, N., et al. (2017). *Using a Real-Time Cybersecurity Exercise Case Study to Understand Temporal Characteristics of Cyberattacks*. International Conference on Social Computing, Behavioral-Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation. Springer, pp. 127–132.

Rossman, G. B. & Wilson, B. L. (1985). Numbers and words: Combining quantitative and qualitative methods in a single large-scale evaluation study. *Evaluation Review 9*(5), 627–643.

Roy, S., Das, S. K., & Xue, M. (2020). 15 Wide-Area Management of Cyber-Physical Infrastructures: A Call to Action. Principles of Cyber-Physical Systems: An Interdisciplinary Approach, p. 417.

Saaranen-Kauppinen, A. & Puusniekka, A. (2009). Menetelmäopetuksen tietovaranto KvaliMOTV. Kvalitatiivisten menetelmien verkko-oppikirja.Yhteiskuntatieteellisen tietoarkiston julkaisuja.

Sabillon, R., Cavaller, V., & Cano, J. (2016). National cyber security strategies: Global trends in cyberspace. *International Journal of Computer Science and Software Engineering 5*(5), 67.

Sahlberg, P. & Leppilampi, A. (1994). Yksinään vai yhteisvoimin?: yhdessäoppimisen mahdollisuuksia etsimässä. Helsingin yliopisto, Vantaan täydennyskoulutuslaitos.

TSK (2018). Kyberturvallisuuden sanasto, TSK 52, Sanastokeskus TSK ry, Helsinkieacea

Scriven, M. (1966). Social Science Education Consortium. Publication 110: The Methodology of Evaluation.

Sevgi, L. (2003). EMC and BEM engineering education: Physics-based modeling, hands-on training, and challenges. *IEEE Antennas and Propagation Magazine 45*(2), 114–119.

Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cyber security strategies. *International Journal of Computer Science and Information Security 14*(1), 129.

Shannon-Baker, P. (2016). Making paradigms meaningful in mixed methods research. *Journal of Mixed Methods Research 10*(4), 319-334.

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information 22 (2), 63–75.

Siemens, G., & Conole, G. (2011). Connectivism: Design and delivery of social networked learning. *International Review of Research in Open and Distance Learning 12*(3).

Sinha, K. (2014). Structural complexity and its implications for design of cyber-physical systems.

Skirpan, M. (2018). Quantified Self: An Interdisciplinary Immersive Theater Project Supporting a Collaborative Learning Environment for CS Ethics.

Steffens, K. (2015). Competences, learning theories and MOOCs: Recent developments in lifelong learning. *European Journal of Education 50*(1), 41–59.

Subaşu, G., Roşu, L., & Bădoi, I. (2017). *Modeling and Simulation Architecture for Training in Cyber Defence Education*. 2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), pp. 1–4.

Švábenský, V. (2020). What Are Cybersecurity Education Papers About?: A Systematic Literature Review of SIGCSE and ITiCSE Conferences.

Tabassum, M. (2018). Evaluating Two Methods for Integrating Secure Programming Education.

Tashakkori, A., Johnson, R. B., & Teddlie, C. (2020). *Foundations of Mixed Methods Research: Integrating Quantitative and Qualitative Approaches in the Social and Behavioral Sciences*. Sage Publications.

Tashakkori, A., Teddlie, C., & Teddlie, C. B. (1998). *Mixed Methodology: Combining Qualitative and Quantitative Approaches*. Sage.

Taylor, C., Arias, P., Klopchic, J., Matarazzo, C., & Dube, E. (2017). {CTF}: *State-of-the-Art and Building the Next Generation*. 2017 {USENIX} Workshop on Advances in Security Education (ASE; 17).

Thomas, L., Deaudelin, C., Desjardins, J., & Dezutter, O. (2011). Elementary teachers' formative evaluation practices in an era of curricular reform in Quebec, Canada. *Assessment in Education: Principles, Policy & Practice 18*(4), 381–398.

Törngren, M. & Grogan, P. T. (2018). How to deal with the complexity of future cyber-physical systems? *Designs* 2(4), 40.

Tynjälä, P., & Collin, K. (2000). Koulutuksen ja työelämän yhteistyö–pedagogisia näkökulmia. *Aikuiskasvatus 20*(4), 293-305.

Vähäkainu, P., Lehto, M., & Kariluoto, A. (2020). *IoT–based Adversarial Attack's Effect on Cloud Data Platform Services in a Smart Building Contex*t. Teoksessa International Conference on Cyber Warfare and Security, pp. 457–465.

Van Maanen, J., Sørensen, J. B., & Mitchell, T. R. (2007). The interplay between theory and method. *Academy of Management Review 32*(4), 1145-1154.

Van Weert, T. J. & Kendall, M. (2006). *Lifelong Learning in the Digital Age: Sustainable for All in a Changing World*. Springer.

Vigna, G., Borgolte, K., Corbetta, J., Doupe, A., Fratantonio, Y., et al. (2014). *Ten Years of ICTF: The Good, the Bad, and the Ugly*. 2014 (USENIX) Summit on Gaming, Games, and Gamification in Security Education (3GSE, 14).

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P. & Tovarnak, D. (2017). *Lessons Learned from Complex Hands-On Defence Exercises in a Cyber Range*. 2017 IEEE Frontiers in Education Conference (FIE), pp. 1–8.

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security 27*(5), 781–799.

Woodley, A. (2004). *PREST in Open and Distance Learning: Getting and Analysing Quantitative Data* (A3 module). Commonwealth of Learning (COL).

Xu, L., Huang, D., & Tsai, W. (2013). Cloud-based virtual laboratory for network security education. *IEEE Transactions on Education 57*(3), 145–150.

Yamin, M., Katt, B. & Gkioulos, V. (2019). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security* 88, 101636.

ORIGINAL PAPERS

I

CYBER SECURITY EXERCISE – LITERATURE REVIEW TO PEDAGOGICAL METHODOLOGY

by

Jari Hautamäki, Mika Karjalainen, Timo Hämäläinen & Päivi Häkkinen, 2019

INTED 2019: 13th Annual International Technology, Education and Development Conference, Proceedings (pp. 3893-3898). IATED.

DOI: 10.21125/inted.2019.0985

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

II

PEDAGOGICAL ASPECTS OF CYBER SECURITY EXERCISES

by

Mika Karjalainen, Tero Kokkonen & Samir Puuska, 2019

2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
(pp. 103-108). IEEE.

DOI: 10.1109/EuroSPW.2019.00018

Pedagogical Aspects of Cyber Security Exercises

Mika Karjalainen, Tero Kokkonen, Samir Puuska
Institute of Information Technology
JAMK University of Applied Sciences
Jyväskylä, Finland
email: {mika.karjalainen, tero.kokkonen, samir.puuska}@jamk.fi

***Abstract*—Cyber security exercises (CSE) are complex learning experiences aimed at developing expert knowledge and competence through simulation. In this paper we examine pedagogical issues relating to CSE, from exercise design to training results and evaluation. In addition, we present a Deliberate Practice - oriented view on expert and competence development for CSEs. We use data gathered from multiple CSE cases, where we have collected field notes, observations, questionnaire results, and other documentary data while organizing these training events.**

Based on our observations and analysis, integrating pedagogical knowledge and focus with each phase in the CSE lifecycle, i.e. planning, implementation, and feedback phases, the training effectiveness can be improved. We also note that CSE evaluation requires systematic measurements of change ranging from customer experience to organizational change. We also outline avenues for further work relating to various aspects of expert knowledge development and training evaluation in the context of CSEs.

***Index Terms*—cyber security exercise, expert performance, collaborative simulation, simulation pedagogy**

I. Introduction

Cyber security exercises (CSE) are increasingly seen as an important part of personnel training in both commercial and governmental contexts. At present, there exist a gap in research as to how these live exercises should be organized around competence development.

In this paper we present a competence development oriented view on CSE lifecycle, and examine how different components of an exercise could benefit from targeted learning outcomes. We also outline common challenges that often present themselves during various parts of the exercise lifecycle.

JAMK University of Applied Sciences has operated cyber security research, training and development center JYVSECTEC (Jyväskylä Security Technology) since 2011 [1]. JYVSECTEC has conducted the Finland's national cyber security exercise annually since 2013 [2] and, in addition, a large number of different types of CSEs for authorities and companies with critical infrastructure. The Ministry of Defence of Finland announced JYVSECTEC cyber range as a national range in the European Defence Agency's Cyber Range project [3]. Typical number of participants in a national exercise is between 100 to 150 people. Commercial companies operating in critical infrastructure sectors are often exercising with their partners or subcontractors. These exercises typically involve 50 to 100 people. SMEs with their partners usually have 10 – 30 participants in live exercises. When Capture-the-Flag or digital forensics and incident response exercises are held, there are normally 10 to 20 participants. In the past 8 years approximately 1,500 people have participated in the exercise sessions at JYVSECTEC. The data for this multiple-case design comes from documentary data, field notes, observations, and questionnaire results the authors have collected from organizing live CSEs at JYVSECTEC.

The aim of this research is to gain more detailed understanding of the pedagogical principles when using the CSE as a method to educate individuals and organizations to understand the cyber domain. For understanding the overall complexity of cyber domain, the need for CSEs has increased rapidly [4], [5]. Many countries have built up their cyber range facilities, and the latest projects have been aimed to interconnect the existing ranges for arranging mutual exercises between countries [6].

Traditionally, the field of engineering education emphasizes the need of training to learn and apply it in practice. Therefore, in engineering education different types of learning environments simulating real operating environments or facilities have been used as a learning tool for decades. In the field of ICT, information network laboratories and project-based learning environments have been widely used especially in applied software engineering. The current cyber security environment has brought new challenges to teaching. By using traditional teaching environments, it has been possible to teach the areas of expertise that the cyber security expert needs in necessary detail. However, the current environment requires a more holistic approach that integrates discrete skills and fosters understanding of the whole landscape, so that the importance of cause-and-effect relationships in the whole cyber context are understood. From the point of pedagogical frameworks, research related to simulation environments has been made especially in the applied health simulation teaching [7]–[9]. These studies are also applicable to cyber security teaching, but further need for applied research, especially of using cyber range as simulation environment, is obvious.

Lehto et al. [10] highlighted that in the research of cyber security the human factor is missing almost completely in the current literature. The importance of human sciences in technology developmental and cross-disciplinary cyber security issues research is still very limitedly understood. Thus, this research is focused specifically to the pedagogical factors of CSEs, and developing more detailed understanding on how the CSEs should be utilized in cyber security skills education.

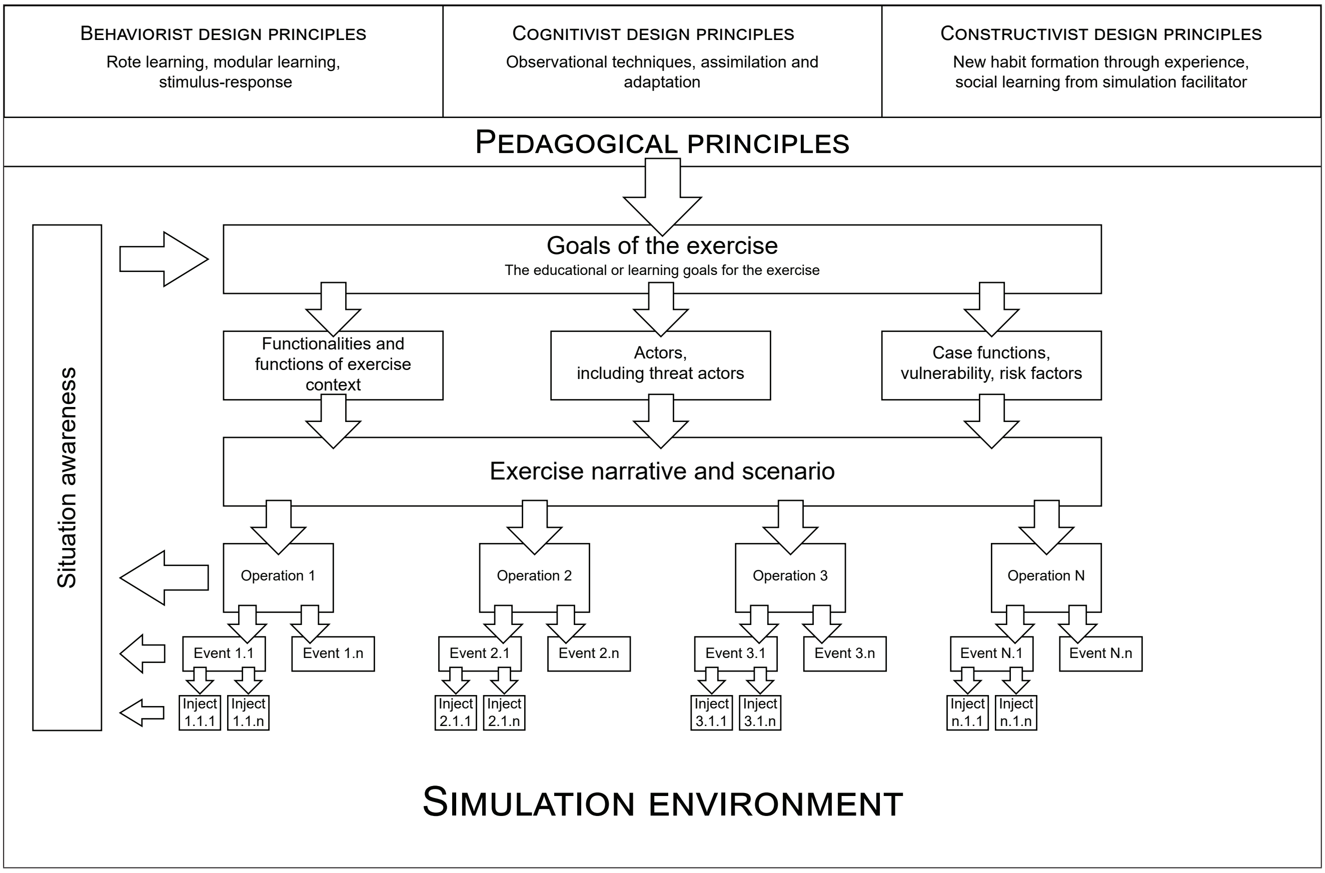

Behaviorist design principles
Rote learning, modular learning, stimulus-response
Cognitivist design principles
Observational techniques, assimilation and adaptation
Constructivist design principles
New habit formation through experience, social learning from simulation facilitator
Pedagogical principles
Situation awareness
Goals of the exercise
The educational or learning goals for the exercise
Functionalities and functions of exercise context
Actors, including threat actors
Case functions, vulnerability, risk factors
Exercise narrative and scenario
Operation 1
Operation 2
Operation 3
Operation N
Event 1.1
Event 1.n
Event 2.1
Event 2.n
Event 3.1
Event 3.n
Event N.1
Event N.n
Inject 1.1.1
Inject 1.1.n
Inject 2.1.1
Inject 2.1.n
Inject 3.1.1
Inject 3.1.n
Inject n.1.1
Inject n.1.n
Simulation environment

Fig. 1. Cyber exercise simulation environment and the content of exercise life-cycle sections.

II. Pedagogy in Cyber Security Exercises

Live CSEs are mostly used to train or assess experts. This means that in order to create efficient learning environments we must understand how expertise works, and which training methods will provide increase in expert performance [11]. Ericsson, in their theory of deliberate practice (DP), argued that this specialized form of practice is necessary component if increase in expert performance is desired [12]. According to Ericsson, experts need well thought-out and specified goals that seek to improve a particular area of their domain. Ericsson argues that experts will not benefit or improve, if the tasks can be accomplished in an automated fashion; in other words, if conscious control is not required the expert can not spot what they should improve. Since DP is aimed at developing expert knowledge, it seems plausible that people who have not attained the highest level on Miller's pyramid [13] of competence lack the necessary experience to fully benefit from this approach.

Skills are often built with lecture-like teaching in the sense of behavioral learning, where the importance of the teacher's lecture material is central. When a student's knowledgeable capacity grows, their cognitive data processing increases, and the student ties in information he has learned earlier, selects the application of knowledge and builds meanings. This is cognitive learning approach that needs to be present when building the deeper knowledge of a subject [14]. In accordance with constructivist learning approach, commonly used learning and teaching methods are problem based learning (PBL) and exploratory learning [15], [16]. Problem based learning often starts directly with solving a real problem and exploring the related background information. Exploratory learning uses the same method. The idea is to react to learning as a researcher. The idea is to set meaningful and interesting questions from the topic to be learned and then solve them. Problem-based teaching practically resembles scientific research. Theoretical parsing of learning places the focus to be on the communities and networks, as well as in the learning and interaction therein, rather than the individual. At CSE, the pedagogical frame of the exercises is based on all these different pedagogical approaches and on combining the needed elements from the different stages of know-how building process (Figure 1). From the perspective of constructivist approach to learning this means that a participant in CSE needs to have a sufficiently high level of competence to be able to tie the educational objectives of the exercise to previously acquired knowledge. European Qualifications Framework (EQF) [17] describes eight different levels of learning outcomes. These learning outcomes consist of knowledge, skills, responsibility and autonomy. Competence is defined by EQF as the proven ability to use knowledge, skills and personal, social and/or methodological abilities in work or study situations.

III. Exercise Life-cycle

Cyber security exercise can be seen as a three phase process [18]: (i) planning phase that identifies the scope and objectives for the exercise, (ii) implementation, the exercise conduct phase where the plans are realized, and (iii) feedback, an evaluation phase where the whole process is analyzed and improved. The stages are also congruent with the stages described by MITRE [19] *Exercise Planning, Exercise Execution and Post Exercise*. Furthermore, the Homeland Security Exercise and Evaluation Program (HSEEP) which provides a set of guiding principles for exercise programs has similar phases, i.e. *Exercise Design, Exercise Conduct and Evaluation* [20]. In essence, each stage is affecting the other as exercises are held repeatedly. Moreover, we have observed that in practice the first two stages will overlap.

A. Planning Phase

The first stage, from a competence development standpoint, determines how effective and useful the later stages are. Almost in all cases, the exercise needs to be scoped to fit a certain subset of an organization.

Figure 1 illustrates how the exercise goals are derived from the pedagogical principles. Based on the desired learning outcomes and the organization in question, various exercise parameters are extracted from the goals and formulated into the exercise narrative. The goals will also define the operational environment (functionalities, threat actors, risks and vulnerabilities) that is to be included in the scenario. This scoping defines the simulation environment that has to be created for the exercise. The exercise scenario is further divided into discrete events and injects. They describe in detail what activity is going to be simulated during the run of a CSE. It is crucial that the role for each person participating in the exercise is well defined. There are several ways of constructing the game scenario, but it is often based on factors such as the threat model, available personnel, and specific skills or capabilities that have been selected after deliberation. The link between a game's scenario and the desired learning outcomes should be detailed at the level where each element and event in-game can be tied to a specific learning goal. Various frameworks have been created to categorize personnel and skills. For example, the NIST's NICE Framework [21] offers lists of specialty areas, work roles, tasks, skills, and abilities for constructing adequately detailed plans. This also allows creating a technical environment that serves the goals. If the plan is not accurate or detailed enough, the resulting technical environment is not tuned to support DP, and may fail to increase expert performance.

All of the above provide technical requirements that should be fulfilled when placing the attendee into a pedagogical situation such as a CSE. If the planning fails to produce detailed plans, the resulting technical environment might not develop the attendees' competences as expected.

Even though the technical environment might be on-par with the plans, the organization of the exercise into teams and responsibilities might fail. We have observed that the teams might (given the freedom) organize themselves less than optimally, and technical injects might not be detected. This can be remedied by the organizer; however, it sometimes lowers the motivation of the participant(s).

Planning a large-scale live CSE is a complex task where various constraints, such as money, planning time, availability of experts, and other practical factors limit the available resources. The process involves interviewing various persons, especially in cases where the exercise organizers are not domain experts on the field, e.g. military or aviation, and require additional support from the organization that contracted them. We have observed that these interviews have difficulties in maintaining their focus and scope, which degrades the quality of communication leading to suboptimal results. It seems likely that methods such as the semi-structured interview could improve the quality of communication, thus improving the results. In terms of future research, it would be beneficial to develop such a framework for CSE purposes.

B. Implementation Phase

The implementation phase differs from the other two stages in many crucial ways. Firstly, the time span for this stage is usually between one to five days. Secondly, the focus is on directing the exercise in a way that all planned objectives are achieved. This introduces the need for maintaining situation awareness (SA) on the exercise at all times. Moreover, since SA is an integral part of expertise, it is usually included in the list of skills that are under training [22], [23]. In other words, one of the challenges in conducting CSEs is in maintaining overall SA on the experts' SAs under training. SA allows the white team (WT) to observe the participants' decisions concerning all the operation lines. At this point, it is crucial also to verify the events and incidents handling from the participants' side. If it seems that participants are not responding to the incidents the way that the goals of learning are fulfilled, the WT will adjust the incidents in a way that the learning goals are reached. The most common way of doing this is to launch new planned incidents that will bring the needed information for the participants and practically guide them towards the set learning goals.

Classical model for decision making in tactical environment is Boyd's OODA loop (Observe-Orient-Decide-Act). Especially the modified version of OODA loop that regards the individuals' background and previous experiences in the Orient phase suits for decision making in cyber domains [24]. Authors of [25] have introduced the cognitive model of OODA loop that improves the level of granularity by considering Endsley's Situation Awareness theory [26] and Klein's Recognition-Primed Decision model [27]. These theories provide the basic for decision making and expertise including learning in stressful and complex CSEs.

In their paper, Lif et al. have studied information elements that should be used in the cyber-incident report during the exercises for a certain professional role known as log analyst [28]. That kind of element focusing can also be used for the competence development for certain roles in the exercises.

C. Feedback Phase

From the perspective of individuals' learning, the feedback phase is most important phase of the exercise. Thus, sufficient time should be reserved for feedback phase. In the feedback phase, all the main operation lines and events have to be gone through. This allows the participants to ask questions concerning the events that they have been phased during the exercise. In many cases it is essential to go into the details of certain incidents and explain how they had been executed, how the participants had responded and what else they could notice or do concerning the incidents. This allows the needed reflection for the participants and leads to understanding and hopefully to achievement of the set learning objectives. Based on our experiment, all the different actors of exercises need to participate in the feedback phase.

IV. Assessing Performance and Results

Evaluation is needed for assessing the effectiveness of a training program [29]. Kirkpatrick has divided program evaluation into four levels: (i) reaction, (ii) learning, (iii) behavior, and (iv) results [30]. The first level, reaction, is the reaction of the participants towards the training. Kirkpatrick characterizes this level as akin to "customer satisfaction". At this level Kirkpatric proposes that forms could be used for estimating how participants felt about the training event [30]. The second level, learning, is defined as the participants improving their knowledge, skills, or attitudes. Kirkpatrick et al. recommend using control groups and tests for assessing learning. They also note that measuring learning is more difficult and time-consuming than reaction measurement [29]. The third level, behavior, refers to the transfer of learned knowledge and skills to actual change in behavior at the actual job or task the participant does at their workplace. Kirkpatrick et al. note that this transfer is hard to measure, in part because the change is not instant; the individual has to have an opportunity for utilizing what they have learned. They recommend using surveys and interviews for assessing if behavioral changes have occurred, after adequate amount of time has passed from training event. The fourth level, results, refers to the final results that occurred because of the training program. These include increases in quality and productivity, and ultimately general return of investment from the training. Kirkpatrick et al. note that assessing these effects is difficult, and much of the same recommendations as for level three are applicable here. They also mention that absolute proof may not be cost-effective to obtain; instead the circumstantial evidence should suffice. [29], [30]

In CSEs the reaction measurements can be made using questionnaires. In addition to customer satisfaction forms, we have, on occasion, included other assessment tools such as the NASA Task Load Index (TLX) [31] for additional measurement. These provide a picture on customer opinion and whether the exercise was demanding enough for its purpose considering the desired learning outcomes. The tools have revealed that much care should be placed to task load planning. Although it may not be appropriate to equalize task loads between participants, there should be more than an occasional task for everyone.

Level two, learning, is considerably more challenging to measure in cyber training contexts. In expert training a simple written test, as Kirkpatrick et al. recommend as a practical instrument, is not applicable. It seems plausible that a more open questionnaire could provide more insight on what has been learned, and further aid in assessing if learning outcomes were met. This questionnaire could be drafted in exercise design phase to reflect the selected learning outcomes. The challenge is in creating a questionnaire that can reliably be used in assessing expert learning. An online evaluation for this level may be feasible, but the details remains a topic for further reseach.

Level three, behavior, is even more challenging to measure. We believe that in a frame of just one exercise there is no way to measure long term effects like changes in behavior, in part because the changes are not immediate; the individual needs time to utilize newly learned matters, and then be able to apply them in a real-world situation in order for them to turn into behavioral patterns. Nevertheless, measuring behavioral changes remains important aspect of any training program's result, as Kirkpatrick et al. point out. A feasible way of doing this assessment would be interviewing people when they return to participate next training program. One major obstacle here is that often there is a need to train persons who were not present in the first program. Questionnaires, both online and offline, may not be flexible enough for measuring training at this level. Semi-structured interviews with key personnel before the next training cycle could provide some insights on behavioral changes.

Level four, results, is the hardest level to assess also in cyber security training context. Agrafiotis et al. have created a taxonomy of "cyber-harms" [32]. They have identified five main harm types: (i) physical and digital harm, (ii) economic harm, (iii) psychological harm, (iv) reputational harm, and (v) social and societal harm. All of these types should be taken into account when assessing what positive effects and, ultimately, results one gets by participating a particular training program.

It is worth repeating that many of the assessments Kirkpatrick et al. recommend are only possible if training is repeated. In other words, a continuous training cycle allows organizations to truly assess how the training benefits them. This observation has been made also in the Cybersecurity Strategy of the European union, and the national cyber security strategy of Finland, among others [33], [34].

V. Conclusion

When dealing with cyber domain, the complexity of the operating environment and the predictability of causal and consequence relationships must always be taken into account. When it comes to teaching skills needed in this environment, the learning environment should be as realistic as possible. Thus, high demands are placed for the simulated environment in CSEs. The environment must therefore be of a sufficiently high standard and allow the needed complexity and realism. If the requirements for a simulated operating environment can be met, CSE is an excellent learning tool for cyber professionals.

As we introduced in exercise lifecycle section, the learning goals of exercises should be considered at all stages of the exercise life cycle. In the planning phase, the objectives of the exercise learning are determined in accordance with the objectives set the operational lines enabling the learning goals set for the participant to be implemented during the implementation phase, and the feedback stage ensures that all learning is possible through detailed level. It is also advisable to allow the material to be shared from the exercise so that the participants are able to return for the details after the exercise. Too often, CSEs focus on technical phenomena without considering what the primary goals set for the exercise are. In an exercise this way executed, the experience of the participants may be left behind to identify the specific technical phenomena instead of the learning that is being targeted. When the learning goals of the exercises are set, a commonly accepted frame such the NICE frame should be used. Using the frame enables a consistent structure implementation of the learning outcomes in the internal structure of exercise; namely, functionalities, processes, threat actors and determination of risk factors, different operation lines, event and inject that are being executed in exercise.Future research should focus on the levels of learning and behavior in Kirkpatrick taxonomy in the context of CSEs. Even though it is important to focus on the individual, the organizational focus should not be overlooked. Accordingly, it is vital to study how CSEs change the behavior of both the individual and and the organization, and ultimately, the cyber resilience capability of the whole society.

References

[1] JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC, “Jyväskylä security technology,” http://www.jyvsectec.fi/en/, Accessed: 7 February 2019.

[2] Ministry of Defence Finland, “The national Cyber Security Exercise is organised in Jyväskylä - Kansallinen kyberturvallisuusharjoitus KYHA18 järjestetään Jyväskylässä, Official Bulletin 11th of May 2018,” https://www.defmin.fi/ajankohtaista/tiedotteet/2018?9610_m=9314, May 2018, Accessed: 7 February 2019.

[3] Ministry of Defence Finland, “Finland has the leader nation role in the EDA project - Suomelle johtovaltiorooli Euroopan puolustusviraston kyberhankkeessa, Official Bulletin 30th of June 2016,” https://www.defmin.fi/ajankohtaista/tiedotteet/2016?8173_m=7894, June 2016, Accessed: 7 February 2019.

[4] The NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, “Exercises,” https://ccdcoe.org/exercises/, Accessed: 19 February 2019.

[5] B. Uckan Färnman, M. Koraeus, and S. Backman, “The 2015 report on national and international cyber security exercises : Survey, analysis and recommendations,” Swedish Defence University, CRISMART (National Center for Crisis Management Research and Training), Tech. Rep., 2015. [Online]. Available: https://www.enisa.europa.eu/publications/latest-report-on-national-and-international-cyber-security-exercises

[6] European Defence Agency, EDA, “Cyber ranges: Eda’s first ever cyber defence pooling & sharing project launched by 11 member states,” https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, Accessed: 4 February 2019.

[7] S. Nyström, J. Dahlberg, S. Edelbring, H. Hult, and M. Abrandt Dahlgren, “Debriefing practices in interprofessional simulation with students: A sociomaterial perspective,” *BMC Med Educ*, vol. 16, no. 1, May 2016. [Online]. Available: http://dx.doi.org/10.1186/s12909-016-0666-5

[8] C. Kenaszchuk, K. MacMillan, M. van Soeren, and S. Reeves, “Interprofessional simulated learning: Short-term associations between simulation and interprofessional collaboration,” *BMC Med*, vol. 9, no. 1, Mar. 2011. [Online]. Available: http://dx.doi.org/10.1186/1741-7015-9-29

[9] G. D. Erlam, L. Smythe, and V. Wright-St Clair, “Simulation is not a pedagogy,” *OJN*, vol. 07, no. 07, pp. 779–787, 2017. [Online]. Available: http://dx.doi.org/10.4236/ojn.2017.77059

[10] M. Lehto, J. Limnéll, E. Innola, J. Pöyhönen, T. Rusi, and M. Salminen, “Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi,” Prime Minister’s Office, Tech. Rep., February 2017. [Online]. Available: https://tietokayttoon.fi/julkaisu?pubid=17805

[11] H. Collins and R. Evans, *A Sociological/Philosophical Perspective on Expertise: The Acquisition of Expertise through Socialization*, 2nd ed., ser. Cambridge Handbooks in Psychology. Cambridge University Press, 2018, p. 21–32.

[12] K. Anders Ericsson, “Deliberate practice and acquisition of expert performance: A general overview,” *Academic Emergency Medicine*, vol. 15, no. 11, pp. 988–994, 2008. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1553-2712.2008.00227.x

[13] G. E. Miller, “The assessment of clinical skills/competence/performance,” *Academic medicine*, vol. 65, no. 9, pp. S63–7, 1990.

[14] S. Lindblom-Ylänne and A. Nevgi, “The effect of pedagogical training and teaching experience on approach to teaching,” in *11th EARLI conference, Padua*, 2003.

[15] J. R. Savery and T. M. Duffy, “Problem based learning: An instructional model and its constructivist framework,” *Educational technology*, vol. 35, no. 5, pp. 31–38, 1995.

[16] M. Njoo and T. De Jong, “Exploratory learning with a computer simulation for control theory: Learning processes and instructional support,” *Journal of Research in Science Teaching*, vol. 30, no. 8, pp. 821–844, 1993. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/tea.3660300803

[17] Official Journal of the European Union, “COUNCIL RECOMMENDATION of 22 May 2017 on the European Qualifications Framework for lifelong learning and repealing the recommendation of the European Parliament and of the Council of 23 April 2008 on the establishment of the European Qualifications Framework for lifelong learning,” https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017H0615(01)&from=EN, Accessed: 14 February 2019.

[18] N. Wilhelmson and T. Svensson, *Handbook for planning, running and evaluating information technology and cyber security exercises*. The Swedish National Defence College, Center for Asymmetric Threats Studies (CATS), 2014.

[19] J. Kick, “Cyber exercise playbook,” The MITRE Corporation https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf, 2014, Accessed: 19 February 2018.

[20] The Department of Homeland Security (DHS), “Homeland security exercise and evaluation program (hseep),” https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf, April 2013.

[21] W. Newhouse, S. Keith, B. Scribner, and G. Witte, *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*, Aug 2017. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-181

[22] M. R. Endsley, *Expertise and Situation Awareness*, 2nd ed., ser. Cambridge Handbooks in Psychology. Cambridge University Press, 2018, p. 714–742.

[23] P. Ward, A. M. Williams, and P. A. Hancock, *Simulation for Performance and Training*. New York, NY, US: Cambridge University Press, 2006, pp. 243–262, iD: 2006-10094-014.

[24] B. Brehmer, "The dynamic ooda loop: Amalgamating boyd's ooda loop and the cybernetic approach to command and control," in *10th International Command and Control Research and Technology Symposium, The Future of C2*, 2005.

[25] R. Breton and R. Rousseau, "The c-ooda: A cognitive version of the ooda loop to represent c2 activities," in *10th International Command and Control Research and Technology Symposium, The Future of C2*, 2005.

[26] M. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, no. 1, pp. 32–64, 1995.

[27] G. Klein, *A Recognition Primed Decision (RPD) Model of Rapid Decision Making*, 01 1993.

[28] P. Lif, T. Sommestad, and D. Granasen, "Development and evaluation of information elements for simplified cyber-incident reports," in *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, June 2018, pp. 1–10.

[29] D. L. Kirkpatrick and J. D. Kirkpatrick, *Evaluating Training Programs*. San Francisco: Berrett-Koehler Publishers, Inc., 2006.

[30] D. L. Kirkpatrick, "Evaluation of training," in *Training and Development Handbook*, L. R. Graig and L. R. Bittel, Eds. New York: McGraw Hill, 1967, pp. 87–112.

[31] S. G. Hart and L. E. Staveland, "Development of NASA-TLX (Task load index): Results of empirical and theoretical research," in *Advances in Psychology*. Elsevier, 1988, pp. 139–183. [Online]. Available: http://dx.doi.org/10.1016/s0166-4115(08)62386-9

[32] I. Agrafiotis, J. R. C. Nurse, M. Goldsmith, S. Creese, and D. Upton, "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," *Journal of Cybersecurity*, vol. 4, no. 1, Jan. 2018. [Online]. Available: http://dx.doi.org/10.1093/cybsec/tyy006

[33] European Comission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," Feb. 2013.

[34] Secretariat of the Security Committee, "Finland's Cyber security Strategy, Government Resolution 24.1.2013," Jan. 2013.

III

MEASURING LEARNING IN A CYBER SECURITY EXERCISE

by

Mika Karjalainen, Samir Puuska & Tero Kokkonen, 2020

ICETC'20: 2020 12th International Conference on Education Technology and Computers (pp. 205-209). ACM, New York.

DOI: 10.1145/3436756.3437046

Measuring Learning in a Cyber Security Exercise

Mika Karjalainen
JAMK University of Applied Sciences,
Institute of Information Technology,
Piippukatu 2, 40100 Jyvaskyla

Samir Puuska
JAMK University of Applied Sciences,
Institute of Information Technology,
Piippukatu 2, 40100 Jyvaskyla

Tero Kokkonen
JAMK University of Applied Sciences,
Institute of Information Technology,
Piippukatu 2, 40100 Jyvaskyla

ABSTRACT

In recent years, cyber security exercises have established themselves as an integral part of cyber security education. Cyber security professionals usually work as a part of a team that monitors and responds to incidents in the environment. A sufficiently realistic complex learning environment is necessary for collaborative learning at the expert level. Evaluating the learning outcomes of complex exercises is an important task for both assessing how individuals met the learning objectives, and how to improve the exercise to better serve those goals. This requires the assessment of multiple skill and knowledge categories independently. We leveraged the NIST NICE Cybersecurity Workforce Framework as a base for building knowledge categories for questionnaire use. However, the NICE framework is comprehensive and detailed requiring that the areas of competence assessment needed to be simplified for questionnaire use. We summarized the NICE framework into 44 questions addressed to the individuals who participated in the exercise. A web-based questionnaire was used to query 21 participants' skill level before and after the exercise, as well as their familiarity and experience with the topic before and during the exercise. The results indicate that cyber security exercises will increase the knowledge of the participant in the knowledge areas that were present in the exercise. This increase was more prominent in cases where the participant was more likely to recognize, and experience events related to that category during the exercise. Furthermore, we concluded that the NICE framework can be used to assess individual know-how and as a basis for knowledge-related questionnaires.

CCS CONCEPTS

• **Social and professional topics**; • **Adult education**;

KEYWORDS

Cyber security, Education, Competence, Skill, Knowledge, Cyber Arena

ACM Reference Format:
Mika Karjalainen, Samir Puuska, and Tero Kokkonen. 2020. Measuring Learning in a Cyber Security Exercise. In *2020 12th International Conference on Education Technology and Computers (ICETC'20), October 23–26, 2020, London, United Kingdom.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3436756.3437046

ICETC'20, October 23–26, 2020, London, United Kingdom
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-8827-6/20/10…$15.00
https://doi.org/10.1145/3436756.3437046

1 INTRODUCTION

Cyber security exercises (CSE) are an efficient resource for personnel training. There is a long tradition of using laboratory environments in engineering education. Typically, the laboratory environment has been constructed to reflect the phenomenon or operating environment of the subject being taught. Previously the laboratory environment often expressed spotted targets from the bigger entirety. Traditional ICT environments have been used in ICT teaching, for example data network laboratories to teach routing and network protocol design. In pedagogical thinking, the above-mentioned teaching method fits into self-regulated learning (SRL) or self-directed learning (SDL) as well as under the experimental learning theories (ELT) [1]. Over the past decade, cyber security has become one of the key topics in the ICT industry.

Programs in graduate education are slow to respond to the changes in the surrounding society, so there has been a delay in responding to the pedagogical demands of cyber security. When considering the phenomenon of cyber security, the multidimensionality of the phenomena must be taken into consideration. A cyber security professional should be able to master the in-depth details; however, at the same time, professionals should have an understanding of the impact of details on other technologies, processes or functionalities.

This sets specific requirements for the laboratory environment where cyber security education and training will take place. On one hand, it can be said that traditional laboratory environments still have value when teaching the basics or the spotted details of larger environment. On the other hand, a full-scale simulation environment is required, thus in the domain of cyber security cyber ranges have been built to execute cyber security exercises (CSE).

2 BACKGROUND AND RATIONALE

2.1 Andragogy

The theory of andragogy makes a difference in the learning between adults and children [2]. For adult learners, the learning process is described as a self-directed learning process. An adult learner is perceived to be self-directed, able to apply what one has learned in the past and to apply what one has learned to practice [3]. For adult learners, education should induce a distorted cognitive dissonance that breaks the habit of old thinking and generates the desired critical-analytical stage of engaging the learner with new knowledge, opinion or action. Cognitive dissonance theory (CDT) suggests that when learners have two or more cognitions that are conflicting, they will feel a displeasing state – dissonance – until they are able to resolve this state by modifying their cognitions [4]. It can be said that in andragogy theory learning is focused on a hands-on perspective implemented in the context of real-life simulation environment [5].

2.2 Experiential Learning

The theory of experiential learning cogitates that the experiencing alone does not guarantee good learning outcomes; it also requires thinking and conceptualization, such as speech and reflection [6]. Through conceptualization an individual can transform unimaginative and unconscious information into conceptualized and conscious information building. This means that by contemplating an action verbally, the vague blur of experience and emotion becomes a word-made activity that can be understood and transformed to new knowledge. Thus, there must be a lot of reciprocity and discussion between the teacher and the student. A student reveals what he or she is trying to learn by deeds and words, and the teacher responds with a variety of feedback methods, such as advice, criticism, explanation or examples [6–9]. In his theory of deliberate practice (DP), Ericsson argued that a specialized form of practice is a necessary component if the aim is to increase the expert performance is desired [10]. Accordingly, Ericsson´s DP model experts need well-defined learning objectives to develop a specific area of their expertise. Thus, experts should attain the highest level on Miller´s pyramid [11] to fully benefit from CSE as a learning method.

2.3 Collaborative Learning

Collaborative learning (CL) is a pedagogical theory where collaboration and built consensus between the student group members generates learning [12]. Group members take responsibility for their own learning, share their insights and work towards a common goal by solving problems, completing tasks, and thus learning [13]. In order to execute successful group work towards the CL five basic elements should be fulfilled: (i) clearly perceived positive interdependence, (ii) considerable interaction, (iii) individual accountability and personal responsibility, (iv) social skills, and (v) group self-evaluation [14, 15]. CSE can be seen as an application of collaborative learning methodology. The above elements are realized at different stages of the CSE life cycle [16].

2.4 Complex Environments

In the real cyber domain, the interdependencies between different systems, network and data form an extremely complex totality. Cyber incident as one component of that complex domain may affect erratic consequences on other systems or even in a physical domain. When discussing learning environments in cyber security, it must be realized that the realistic training environments shall be complex enough for in order to reflect the sophisticated interdependent relationship of networks, systems and data of the real world. Traditionally, these training environments are called as "Cyber Range". The problem with that familiar term is that the spectrum of cyber ranges is extremely heterogenous varying from simple laboratory-based test beds to complex mimics global Internet. Paper [17] introduces the concept of cyber arena; the next generation cyber range, with its pedagogical viewpoints and technical requirements. As stated in [17],"it is recommended to use the term Cyber Arena when discussing state-of-the-art modern and complex cyber security exercise platform".

2.5 NICE Framework

To manage know how in the domain of cyber security, National Institute of Standards and Technology (NIST) has created National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [18]. This NICE framework can be used to describe the competencies required for various cyber security jobs [19]. Its purpose is to unify the concepts and taxonomies of business, industry and education providers for the cyber content-specific needs in different areas of expertise. The framework can also be applied to define the necessary contents of the core competency of cyber skills and thereby to develop curricula and course content [20].

3 RESEARCH METHOD

The research was carried out in JAMK University of Applied Sciences master's degree program in cyber security [21]. The course uses the comprehensive cyber arena as a training platform that is able to embody key Internet functionalities, as well as the modeled companies' ICT infrastructure and the interdependence between them [17]. The training platform also enables the modeling of the needed complexity, which is a key phenomenon in cyber security education. In the degree program one element of the course is a cyber exercise which is carried out so that students participate in the planning and implementation of the exercise. At the beginning of the course, there is a planning phase where students plan the information security controls of the fictional company's ICT environment.

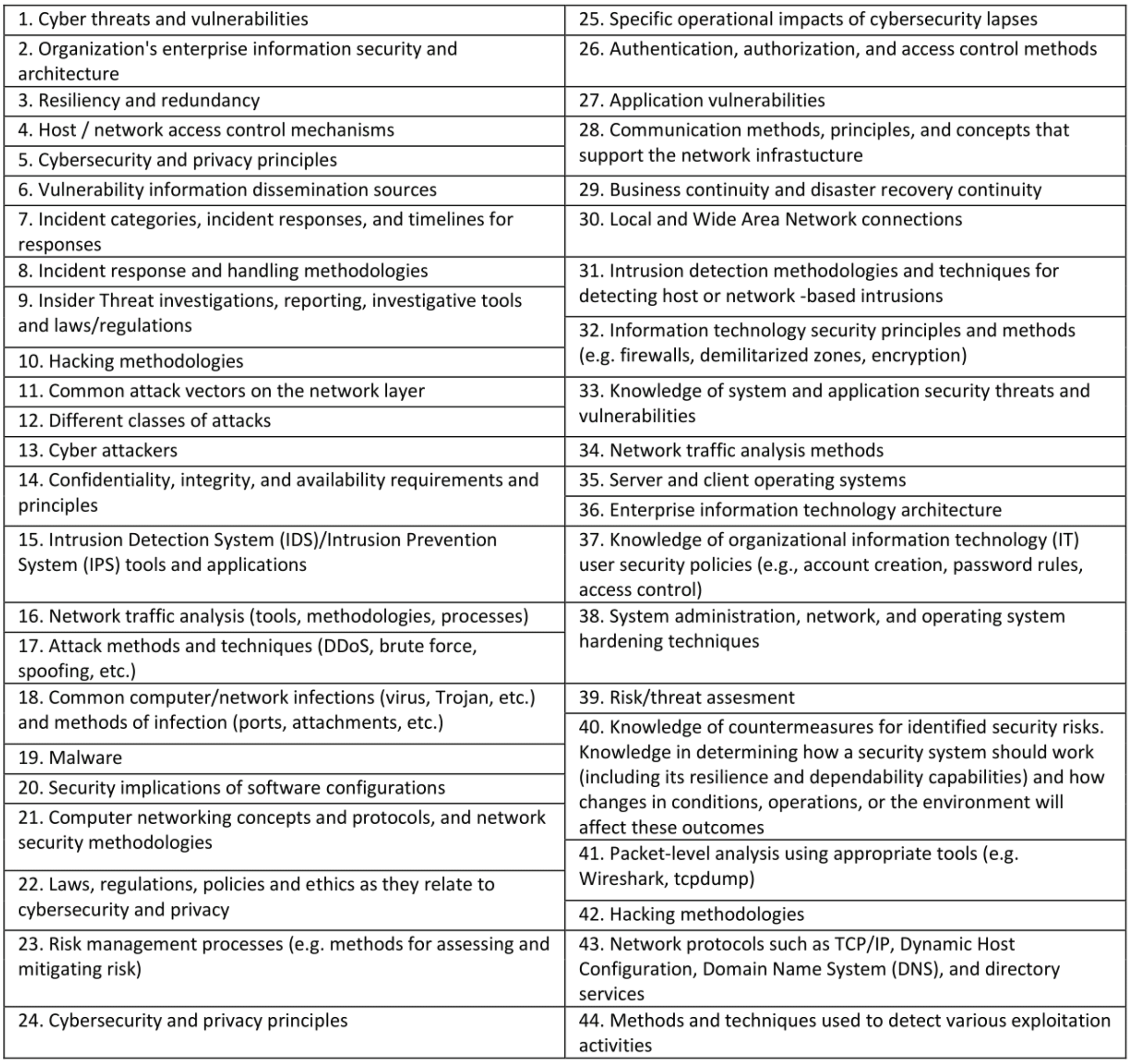
The basics and practices of security control design have been taught and practiced in the previous courses of the degree program. The course proceeds to the active phase of the exercise, which is implemented as so-called blue team cyber security exercise method, where students act as an ICT team of the company´s infrastructure they have built in the design phase. The exercise proceeds according to the planned scenario and lasts approximately two working days. After the active phase of the exercise, the events of the exercise are reviewed, and students write an after-action report of the exercise where they reflect the learning they have reached during the course. We sent the questionnaire via e-mail to 86 persons that participated in the cyber exercise as blue team members. The questionnaire was sent to the students after they had completed the after-action report.

We used the NIST NICE framework as a starting point for creating a questionnaire that captured the key learning elements of a cyber security exercise. In order to leverage the NICE framework, the authors and two other cyber security experts familiar with CSEs ranked the frameworks 630 "Knowledge" related areas of expertise. The ones marked by every author were included as basis for further refinement. They were further distilled by combining overlapping areas into broader categories, resulting in 44 topics overall (Table 1). For assessing knowledge increase we selected a total of five questions addressing the knowledge level before and after the exercise, a question regarding subjective feeling of increased knowledge, and two questions about the topic if it was seen as present and personally encountered during the exercise (table 2).

4 RESULTS

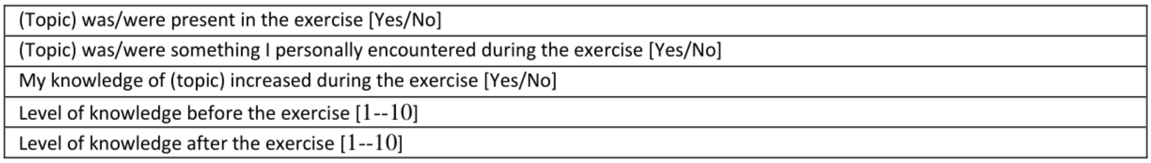
Overall, 21 people submitted answers to all questions. Improvements were seen in almost each category. Figure 1 presents the box

Table 1: List of the topics covered in questionnaire



1. Cyber threats and vulnerabilities	25. Specific operational impacts of cybersecurity lapses
2. Organization's enterprise information security and architecture	26. Authentication, authorization, and access control methods
3. Resiliency and redundancy	27. Application vulnerabilities
4. Host / network access control mechanisms	28. Communication methods, principles, and concepts that support the network infrastucture
5. Cybersecurity and privacy principles	
6. Vulnerability information dissemination sources	29. Business continuity and disaster recovery continuity
7. Incident categories, incident responses, and timelines for responses	30. Local and Wide Area Network connections
8. Incident response and handling methodologies	31. Intrusion detection methodologies and techniques for detecting host or network -based intrusions
9. Insider Threat investigations, reporting, investigative tools and laws/regulations	
10. Hacking methodologies	32. Information technology security principles and methods (e.g. firewalls, demilitarized zones, encryption)
11. Common attack vectors on the network layer	33. Knowledge of system and application security threats and vulnerabilities
12. Different classes of attacks	
13. Cyber attackers	34. Network traffic analysis methods
14. Confidentiality, integrity, and availability requirements and principles	35. Server and client operating systems
	36. Enterprise information technology architecture
15. Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications	37. Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control)
16. Network traffic analysis (tools, methodologies, processes)	38. System administration, network, and operating system hardening techniques
17. Attack methods and techniques (DDoS, brute force, spoofing, etc.)	
18. Common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.)	39. Risk/threat assesment
19. Malware	40. Knowledge of countermeasures for identified security risks. Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes
20. Security implications of software configurations	
21. Computer networking concepts and protocols, and network security methodologies	
	41. Packet-level analysis using appropriate tools (e.g. Wireshark, tcpdump)
22. Laws, regulations, policies and ethics as they relate to cybersecurity and privacy	42. Hacking methodologies
23. Risk management processes (e.g. methods for assessing and mitigating risk)	43. Network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services
24. Cybersecurity and privacy principles	44. Methods and techniques used to detect various exploitation activities

Table 2: List of questions for each topic



(Topic) was/were present in the exercise [Yes/No]
(Topic) was/were something I personally encountered during the exercise [Yes/No]
My knowledge of (topic) increased during the exercise [Yes/No]
Level of knowledge before the exercise [1--10]
Level of knowledge after the exercise [1--10]

plot statistics containing the interquartile ranges (IQR) of answers. The left box plot (red) describes the knowledge before the exercise and the right box plot (blue) the knowledge after the exercise. Inside of the box plot, the median line of the answers can be seen. Small balls or stars outside of the box plots are outlier answers which were out of the corresponding IQR's whisker's max/min 1.5 times IQR. Based on the answers from the questionnaire, it can be stated that the competence level of the respondents generally increased. Notably, the exceptions in the questions where knowhow of the respondents did not increase significantly (questions 21, 25, 26, 28,

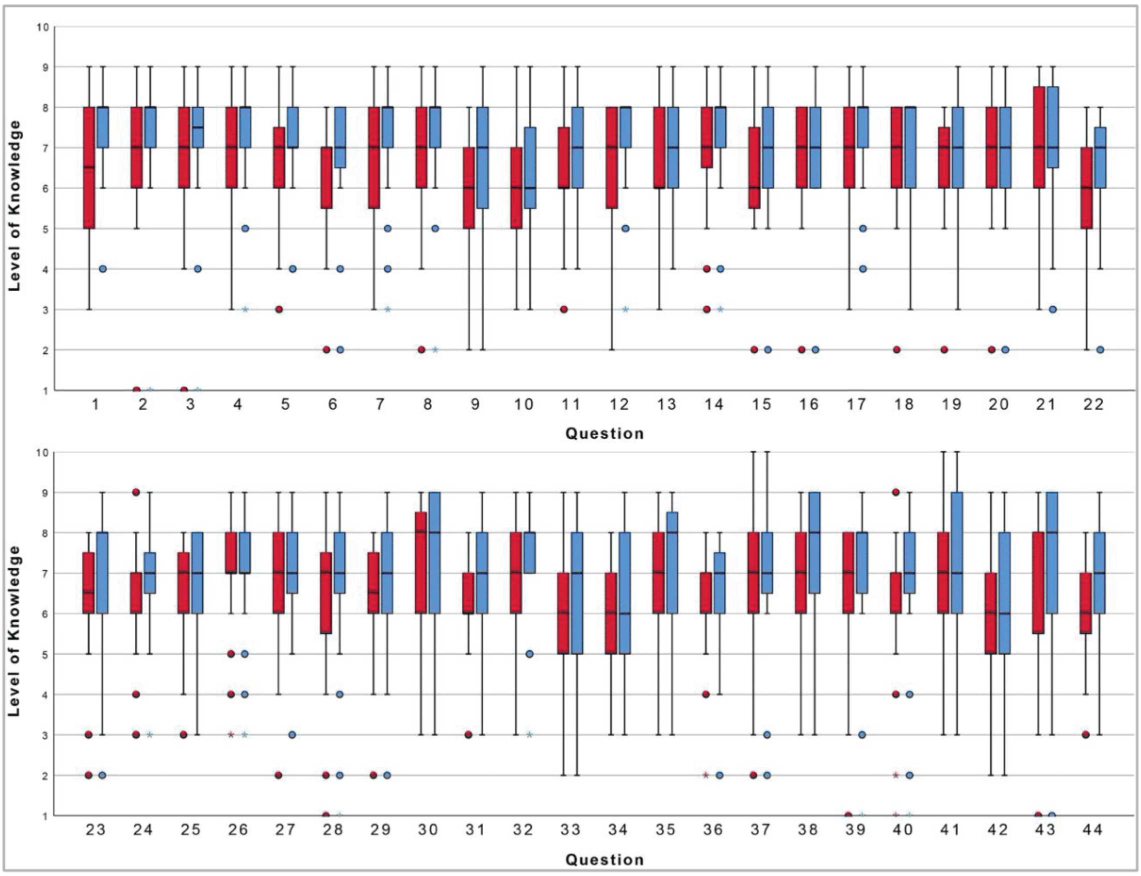


Figure 1: Level of knowledge before and after the exercise

29, 30, 36, 41) were likely due to the fact that the areas of those questions were not prominently present in the exercise where this data was collected. The above observation supports the correlation of responses with the type of exercise that was executed. In overall 36 questions the responses indicated that they had experienced significant learning. The top five areas (questions 1, 2, 7, 8, 33) where according to the questionnaire answers the learning took place the most are the general principles of cyber security, the threats and vulnerabilities on a large scale, and the areas dealing with the security architecture of the organization.

The result shows that cyber security training implemented in a comprehensive cyber range is an excellent teaching method and platform. The exercise can summarize the previous course sections and bring students an understanding of the large complex operating environment which is needed knowledge for cyber security professionals in cyber security domain. The data of the answers shows that participants with a lower level of knowledge achieved greater competence growth. However, the respondents' knowledge level was on average 6-7, which means that the respondents were not beginners for their level of knowhow. It should be noted that the assessment of the person's own knowledge before and after the exercise is a subjective assessment of the person for question; the respondents were not given any baseline test to identify any difference between their own rating and the level of proficiency found in the questionnaire.

Building an objective metric to assess a person's competence remains elusive. This is because the exercise is a very complex environment, where it is challenging to evaluate people who have e.g. different roles. It is also difficult to predict what kind of tasks and difficulty level of the tasks each participant will encounter during the exercise. In this exercise the participant's performance was not scored. This is because we believe that by scoring a participant's activity will begin to guide the participant's activities towards activities that he or she finds to receive more points. The focus of the exercise has been on the development of the individual's skills and knowledge, through when it is possible, to develop also the competence of the organization participating in the exercise.

5 CONCLUSIONS

Based on the conducted research, it can be said that the NICE framework can be used as a baseline for creating questionnaires that measure levels of knowledge improvement. The NICE framework can also be used in a targeted way to measure the competence in a certain substance area. In this paper, a common set of indicators on various aspects of cybersecurity was desired. The used pedagogical theory is not complete. The cyber security exercise is a large pedagogical learning event where various elements are manifested. Some pedagogical phenomena's do not always materialize in practice, so it is almost impossible to build a comprehensive theoretical framework for exercise. However, key theories of experiential learning combined with collaborative learning provide a sufficient basis for the theory. There are also recognizable elements of problem-based learning and exploratory learning frameworks in the exercise, as during the exercise the student acts as a researcher observing the environment and reacting to the findings of the operating environment.

The qualifying was done by a mapping list of questions by experienced teachers and experts, so that only the most relevant questions remained in the final questionnaire. The difficulty with the NICE framework is the level of details in the framework. With a total of 630 knowledge areas alone, the resulting questionnaire would be prohibitively long if they all were included. However, it should also be noted that the framework's knowhow descriptions are at very different levels of details. Some of the knowhow descriptions are very general and some very detailed. This should be taken into account when constructing the questionnaire.

A development proposal for future work would also be the categorization of a list of questions, which would provide a much-needed summary through possible overlaps between different issues. Answering the questionnaire was scheduled at the end of the course so that all the elements influencing learning would been reviewed before answering. Especially the hot wash up event after the exercise is an essential opportunity to review the implemented scenarios and technical elements in different cyber events and / or threat campaigns that have been executed during the exercise. From the learning perspective, the hot wash up event is an important part of the course. It seems that at this stage the students were no longer motivated to answer the question set, which was quite time consuming.

The observation is also corroborated by the phenomenon observed from the data, which addressed that 53 respondents started answering the question set; however, only 21 answered it fully. This indicates that answering the 44 detailed questions is challenging for the respondents. In the future research, we will place answering the question set as part of the course performance, which will hopefully result in a significantly better sampling. Although the number of respondents to the questionnaire set remained relatively low, it can be said that the cybersecurity exercise serves as an excellent wide-ranging learning environment. The learning outcomes were significant in the area of 36 questions from 44. It also seems that possible differences in students' entry levels knowledge do not interfere the learning during the exercise and students will be able to adapt their actions according to their own level of knowledge to perform tasks that enable contributing to the team and thus, they will be able to learn at their own level.

Other studies measuring the development of the knowledge of the students who participated in the cybersecurity exercise have not been conducted with this method.

As future research, we will collect a larger sample, so the sample will be more representative. We will also continue to analyze qualitative interview data that was collected as part of the research. This allows for a more detailed analysis of the phenomena that have now emerged, but which cannot be explained by the quantitative data. Such an observation was, for example, that few of the respondents estimate that their knowhow level would have increased; however, the numerical estimate shows that the respondent had maintained the same knowhow level. In the future, research will be extended to the area of organizational learning. This will be possible utilizing exercises for commercial operators where organizations train their staff on an annual basis.

ACKNOWLEDGMENTS

This research is funded by Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project of the Horizon 2020 SU-ICT-03-2018 program.

REFERENCES

[1] Gemmell, R. M., Boland, R. J., and Kolb, D.A. 2012. The Socio-Cognitive Dynamics of Entrepreneurial Ideation. Entrepreneurship Theory and Practice 36, 5 (2012), 1053-1073.

[2] Knowles, M. S. 1995. Designs for adult learning: Practical resources, exercises and course outlines from the father of adult learning. Alexandria, Va: American Society for Training & Development.

[3] Merriam, S. B. and Bierema L. L. 2013. Adult learning: Linking theory and practice. John Wiley & Sons.

[4] Festinger, L. 1962. A theory of cognitive dissonance. Vol. 2. Stanford university press.

[5] Knowles, M. S. *et al.* 1984. Andragogy in action. Jossey-Bass San Francisco.

[6] Kolb, D. A., Boyatzis, R. E., Mainemelis, C., *et al.* 2001. Experiential learning theory: Previous research and new directions. Perspectives on thinking, learning, and cognitive styles 1, 8 (2001), 227-247.

[7] Engestr√∂m, Y. 2001. Expansive learning at work: Toward an activity theoretical reconceptualization. Journal of education and work 14, 1 (2001), 133-156.

[8] Sch√∂n, D.A. 1987. Educating the reflective practitioner. Jossey-Bass San Francisco.

[9] Malinen, A. 2000. Towards the Essence of Adult Experiential Learning: A Reading of the Theories of Knowles, Kolb, Mezirow, Revans and Schon. International Specialized Book Services.

[10] Ericsson, K. A. 2008. Deliberate practice and acquisition of expert performance: A general overview. Academic Emergency Medicine 15, 11 (2008), 988-994. 2008

[11] Miller, G. E. 1990. The assessment of clinical skills/competence/performance. Academic medicine 65, 9 (1990), S63-7.

[12] Panitz, T. 1999. Collaborative versus Cooperative Learning: A Comparison of the Two Concepts Which Will Help Us Understand the Underlying Nature of Interactive Learning.

[13] Laal, M. 2013. Collaborative learning; elements. Procedia-Social and Behavioral Sciences 83 (2013), 814-818.

[14] Johnson, D. W., Johnson, R. T., Stanne, M. B., and Garibaldi, A. 1990. Impact of group processing on achievement in cooperative groups. The Journal of Social Psychology 130, 4 (1990), 507-516.

[15] Johnson, R. T., and Johnson, D. W. 2008. Active learning: Cooperation in the classroom. The annual report of educational psychology in Japan 47 (2008), 29-30.

[16] Karjalainen, M., Kokkonen, T., and Puuska, S. 2019. Pedagogical Aspects of Cyber Security Exercises. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). IEEE, 103-108.

[17] Karjalainen, M. and Kokkonen, T. 2020. Comprehensive Cyber Arena; The Next Generation Cyber Range. Accepted for 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW).

[18] Paulsen, C., McDuffie, E., Newhouse, W., and Toth, P. 2012. NICE: Creating a cybersecurity workforce and aware public. IEEE Security & Privacy 10, 3 (2012), 76-79.

[19] Newhouse, W., Keith, S., Scribner, B., and Witte, G. 2017. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST Special Publication 800 (2017), 181.

[20] Saharinen, K., Karjalainen, M., and Kokkonen, T. 2019. A Design Model for a Degree Programme in Cyber Security. In Proceedings of the 2019 11th International Conference on Education Technology and Computers (ICETC 2019). Association for Computing Machinery, New York, NY, USA, 3-7. DOI:https://doi.org/10.1145/3369255.3369266.

[21] Master's Degree Programme in Information Technology, Cyber Security. 2019-2021. JAMK University of Applied Sciences. Retrieved August 13, 2020. https://studyguide.jamk.fi/en/study-guide-masters-degrees/studying-at-jamk/curricula/2019-2020/information-technology-cyber-security/

IV

COMPREHENSIVE CYBER ARENA: THE NEXT GENERATION CYBER RANGE

by

Mika Karjalainen & Tero Kokkonen, 2020

2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)
(pp. 11-16). IEEE.

DOI: 10.1109/EuroSPW51379.2020.00011

Comprehensive Cyber Arena; The Next Generation Cyber Range

Mika Karjalainen, Tero Kokkonen
Institute of Information Technology
JAMK University of Applied Sciences
Jyväskylä, Finland
email: {mika.karjalainen, tero.kokkonen}@jamk.fi

***Abstract*—The cyber domain and all the interdependencies between networked systems form an extremely complex ensemble. Incidents in the cyber domain may have an abundance effect on the physical domain. For example, a cyber attack or an intrusion against an electricity system may affect the performance of healthcare system as well. For organisation´s cyber resilience, know-how is the key resource. Cyber security training and exercises have an extremely important role for achieving the required level of know-how in the cyber domain. The old military based-proverb *You Fight Like You Train* is relevant in the cyber domain. Traditionally, the platform for cyber security training and exercises is called *cyber range*. Because of the accelerating digitalisation and more complex totality of the cyber domain, also the infrastructure for the cyber security training and exercises is required to be more and more complex. In this paper, the concept of cyber arena, next generation cyber range, is discussed.**

***Index Terms*—cyber security, cyber security exercise, cyber security training, cyber security exercise platform, cyber range, cyber arena**

1. Introduction

Cyber security as a concept has become more widespread from the early 2010s because the fast growing digital world has brought in new classes of threats. The threats have grown more disruptive, which has led to the need to reassess and redefine the threat they pose to modern society. Naturally, the environmental change has reflected also on the requirements of education. The changes brought by digitalisation must be observed at all levels of education, and eventually digital skills should become part of our daily lives as new civic skills. One of the most important assets in cyber domain is know-how. It is achieved by training and exercises. Finland's new cyber security strategy [1] states that *the high level of education required by nationally critical cyber competence areas will be ensured. This is supported by both national and international training and exercises*. In addition, the cyber security strategy of the European Union [2] recognises the importance of cyber security training and exercises.

Cyber range performs as a technical platform for research & development and training & exercise in the cyber domain. Cyber range simulates the required networks and systems for supporting the research & development or training & exercises. Cyber range is a closed and the controlled environment with the required systems, tools and networks including a realistic Internet simulation with background traffic generation and user simulation. Because cyber range a closed environment, it is risk-free to use realistic cyber security threat environments with real attacks and intrusions [3]–[5].

In the field of training and exercise, cyber range can be equated as classical shooting range with capability to train and develop skills with weapons, operations or tactics [6]. One of the first cyber ranges was developed by the Defense Advanced Research Projects Agency (DARPA). DARPA realised the scientific advances of cyber security and requirements for research and development based on testing and experimentation. They developed the first version of national test bed that was later established as National Cyber Range (NCR) [5]. For example, paper [7] uses NCR as a blueprint of cyber range.

There are numerous different cyber ranges in the world, developed by industry, universities, research centres or national security organisations. The capabilities of those cyber ranges vary from laboratory based one server test bed infrastructures to massive virtualised Internet-kind of infrastructures. Yamin et.al [8] have conducted a literature review of cyber ranges and security testbeds including scenarios, functions, tools and architectures. As stated in [9], cyber ranges are often built for a specific purpose for fulfilling the narrow scale requirements of specific test scenarios. There also exist industry specific cyber ranges or test systems. He et al. [10] introduce a design of a cyber range test system for power industry, while Chen et al. [11] introduce a construction of cyber range in a power information system. Cybertropolis is a United States Department of Defense resource that can be seen as cyber-electromagnetic range including both kinetic and non-kinetic activities [12].

The perspective and requirements for developing the cyber ranges are often narrow and limited to a specific area of interest. Frank et al. [13] state that national cyber ranges are testbeds with command and control functionality, while the authors of [14] state that training environments are often not realistic enough. Paper [15] proposes a tool for creating an emulated network environment for cyber defence exercises while paper [16] introduces an architecture for cyber defence training and education. Cyber range is also effective for research and development activities, for example the authors of paper [17] utilised cyber range for deep learning based network security assessment and indication.

The complexity of networked systems has increased the effect of unexpected behaviours and dependences [18]. In that complex totality it is extremely important to understand what is happening in the cyber domain, what the statuses of the valuable assets are and how different dependencies affect to the valuable assets. In that sense, the Situational Awareness (SA) has an important role in the cyber domain. Debatty & Mees introduce cyber range for training the SA [19]. Because of the different capabilities of different cyber ranges and the growing requirement for simulating the complexity of the cyber domain, the Cyber Defence Pooling & Sharing Project of European Defence Agency (EDA) has recognised requirement for co-operation between national cyber ranges at the European level [20]–[22].

1.1. Motivation and Structure

As can be seen, the spectrum of cyber ranges is extremely heterogeneous and because of the evolution of cyber domain, there is a requirement for simulation of total complex cyber-physical environment with unexpected dependencies and consequences. Because of that, the new concept Cyber Arena (CA) is introduced and discussed.

The paper is organised as follows. In section 2, the pedagogical aspects for a complex system are discussed. According to that, the Cyber Arena (CA) is introduced in section 3. Lastly, in section 4, the study is concluded with emerging future research topics.

2. Pedagogical aspects for complex system

For decades, technical education has utilised learning environments that simulate real environments or functions as a learning tool. Information technology laboratories and project based learning have been widely used in the ICT field, particularly in applied software engineering studies. Cyber security has brought new challenges to ICT education. It has previously been adequate to teach spot-points from the individual areas of expertise using traditional teaching environments. However, by doing so the significance of cause-and-effect relationships will be missed. Furthermore, the learning goals for larger entities, such as an organisation's cyber security entity, may not be achieved. Often the effectiveness between the existing systems or their multiplier effects is difficult to predict and these elements also have to be included into training. From the viewpoint of pedagogical frameworks, research on simulation environments has been conducted, especially regarding the application of simulation teaching in healthcare [23]–[25]. In part, these studies are also applicable to cyber security teaching; however, the need for applied research, especially regarding the training and exercise environments (cyber range) built for cyber security teaching, is obvious.

In order to accommodate the changes driven by digitalisation in education and teaching, we need specific educational environments that model those complexities our societies increasingly rely on. In the digital business environment, it is typical that the in functionalities that are executed, the cause and effect relationships are difficult to understand. On the other hand, it can be said that it is crucial for the success of society and organisations that the skills of experts can be brought to a level where they can operate, develop and solve problems in the modern operating environments. New technologies require new skills from the experts, while the existing legacy systems still require administrator skills. Complex systems that are constantly evolving require risk-free, realistic learning environments where practical training and exercises can be provided for both beginners and advanced experts. It is not enough for knowledge to accumulate, but learning must aim at the level where specialists have the capability to react to real-life situations quickly with the right actions and in the face of ever more complex information entities. It is impossible to learn these skills without addressing these situations during training or exercise. Thus, according to Herrington and Oliver's theory of designing frameworks of authentic learning environments, continuous training is required in authentic learning environments, which refers to the accumulation of knowledge and skills in contexts that reflect the ways and environments where knowledge and skills will be used in real life [26]. The following list describes Herrington and Oliver's designing framework.

1) Provide authentic context that reflect the way the knowledge will be used in real-life
2) Provide authentic activities
3) Provide access to expert performances and the modelling of processes
4) Provide multiple roles and perspectives
5) Support collaborative construction of knowledge
6) Promote reflection to enable abstractions to be formed
7) Promote articulation to enable tacit knowledge to be made explicit
8) Provide coaching by the teacher at critical times, and scaffolding and fading of teacher support
9) Provide for integrated assessment of learning with in the tasks

In addition to the listed design criteria of authentic learning environment, it should be noted that also the pedagogical tasks that are executed in the environment should be designed by Authentic learning theory [27]. Collins [28] defines, that based on the theory of situated learning, when the new skills are learned and practised in an environment that reflects the real-life the new knowledge will also be useful in real life.

3. Comprehensive Cyber Arena

In order to fully achieve the educational goals so that the knowledge is applicable in the real environment, the cyber-training environment should be able to express cyber security phenomena and technology on a large scale. When considering cyber security, the complexity, difficulty to predict causal relationships, accountability, and other ecosystem-related phenomena need to be considered.

In the cyber ecosystem it must be taken into account that the influences and relationships of the actors are very sensitive and complex. For example, a company's cyber resilience consists not only of the security status of its own corporate network, but also of the security level of its partners, subcontractors, customers, service providers, and the critical infrastructure connected to it. In order to these ecosystemic influences to be reflected in teaching, the learning environment requires the ability to model the real environment and its phenomena at a sufficiently realistic level.

When describing cyber security training environments, there is an established term cyber range which is widely used. In their literary review Yamin [8] extensively mapped the existing cyber ranges. Based on Yamin's literature review, it can be said that the term cyber range can include many different uses, technical solutions and functionalities. Thus, the use of the term cyber range should be clarified in order to better identify the purpose, technical implementation or educational objectives of the environment. Many of the cyber ranges mentioned in Yamin's literature review focus on some aspect or functionality of cyber security. In order to be able to teach the ecosystemic influences of the real-world cyber operating environment in a sufficiently realistic operating environment, the training environment must be able to implement most of these functionalities.

An overall figure of Cyber Arena is shown in Figure 1. In Figure 1, Range 1 illustrates a cyber security training environment modelled on a single organisation's ICT architecture and business capabilities, including enterprise IT and OT operations. Range 2 illustrates a cyber security training environment modelling the ICT architectures of two or more organisations, enterprises' business as well as enterprise interdependences of ICT architecture and business. Range 3 illustrates a cyber security training environment modelling internet architecture and the different tier levels internet, enterprise business and ICT architecture, and the cloud architecture that is supporting the business. Range 4 illustrates a cyber security training environment which has the internet architecture, as well as the services used over the Internet and the cloud service architecture. National Initiative for Cyber security Education (NICE), led by the National Institute of Standards and Technology (NIST), has created a framework for managing the industry-based know how in the domain of cyber security [4]. The NICE framework boxes exemplify the positioning of certain NICE knowhows in different areas of Cyber Arena. The goal of the NICE boxes is to embody the manifestation of cybersecurity expertise across the cybersecurity ecosystem. It should be noted that the various range types exemplified in the figure can also be modeled by combining the functions differently than what is presented in the figure. The main argument is that when teaching the functionality of the cyber ecosystem, one should be able to model the ecosystem extensively. Once the ecosystem has been comprehensively modeled, the educational requirements of different knowledge areas of expertise can also be met.Once the ecosystem has been comprehensively modeled, the educational requirements of different knowledge areas of expertise can also be met.

3.1. Requirements of Comprehensive Cyber Arena

To achieve the capability for complex training environment in cyber security domain, following high-level requirements shall be fulfilled. Detailed technical requirements of specific technical implementation can be derived according to these requirements.

3.1.1. Realism. *Cyber Arena shall reflect the complexity and interdependences of real cyber domain.* Theory of authentic learning sets the central principle that the teaching environment is adapted to the environment where the learned know-hows will be practically used. One of the key challenges in cyber security education is to be able to express the difficult predictability of the causal relationships in the complex operating environment, so the Cyber Arena should be able to reflect the trainee's activities elsewhere in the ecosystem.

3.1.2. Isolated and controlled environment. *Cyber Arena shall be an isolated and controlled environment.* For allowing risk free usage of different attack vectors with real attacks and malware without jeopardising production environments, the Cyber Arena shall be isolated and centrally controlled. The national criminal laws of many countries prohibits the dissemination or processing of real malwares. Therefore, a closed environment must be in place to ensure the security and legality of training and exersices.

3.1.3. Internet simulation. *Cyber Arena shall simulate global Internet with its structures and services.* Global Internet is one of the main assets in the cyber domain. By simulating the main services and structures of the Internet, Cyber Arena has much more realism than just simulating some specific network infrastructures. Internet simulation offers the global environment for training and exercises with for example social media applications and usage of Internet based attack vectors. That Internet simulation shall also have the capability to simulate TOR network with Dark-Web capabilities. As said in [29] *"Simulation on Internet services adds the realism of scenarios being implemented by the cyber range. Modern attacks utilise global infrastructure and services considerably in order to avoid detection. Therefore, it is very important for cyber ranges nowadays to be able to simulate the Internet and its services realistically. However, in many cases, Internet services are not simulated due to the added complexity required in order to guarantee the right level of realism."*

3.1.4. User and network traffic generation. *Cyber Arena shall have the capability of network traffic simulation.* As part of the centralised control of Cyber Arena, there shall be the capability to generate network traffic from users and applications. With this capability the Cyber Arena will have ongoing network traffic as in the real networks. Simulated network traffic shall contain for example web-browsing, video streaming, remote-disk traffic, traffic from office software and e-mails. During the trainings and exercises that simulated network traffic allows usage of different attack vectors as in the real cyber domain, for example usage of hidden command and control channel, or some of the simulated network users can be part of distributed denial of service campaign.

3.1.5. Attack execution and simulation. *Cyber Arena shall have the capability of attack execution and simulation.* As part of the cyber security trainings and exercises it is important to execute and simulate attacks. As described earlier, an isolated environment enables the usage of real attacks and malware, in addition to real man made attacks

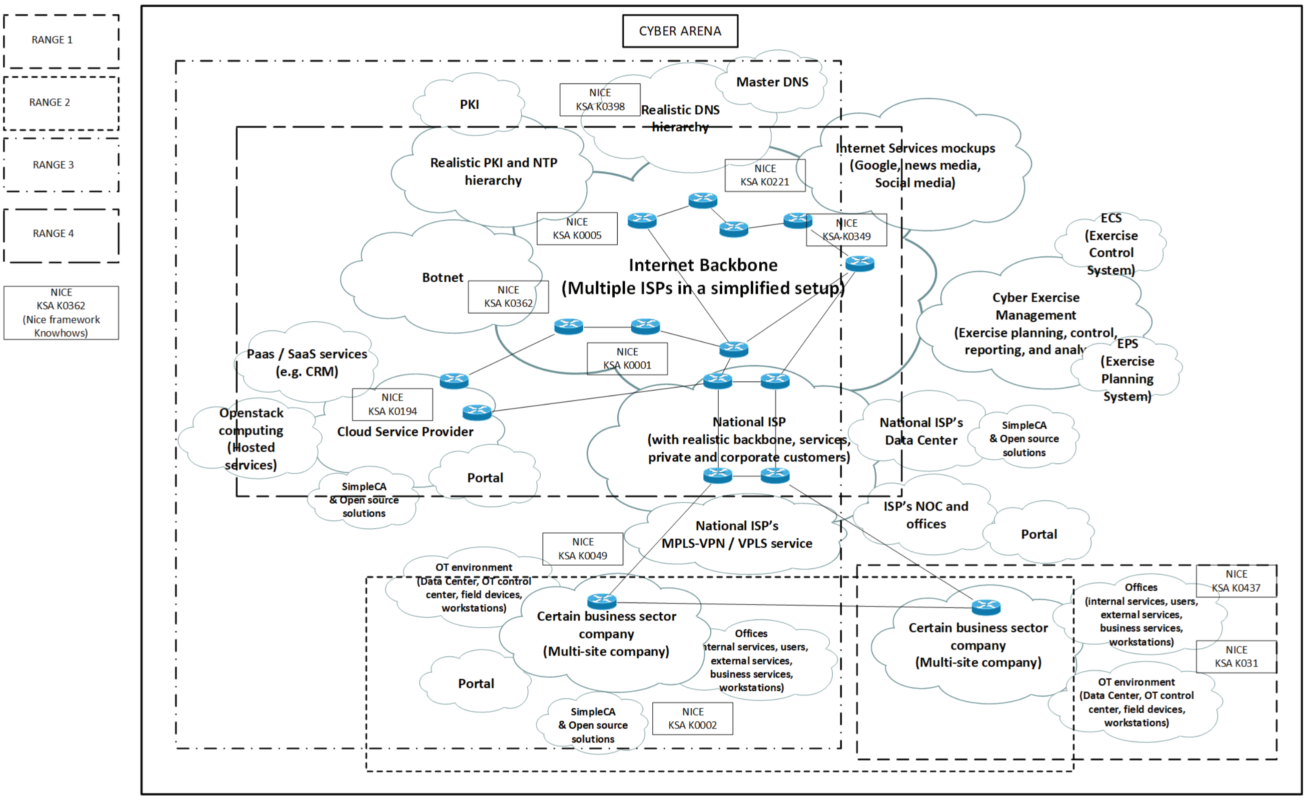


Figure 1. Comprehensive Cyber Arena

some of those can also be simulated. Attack simulation can also be a part of the user and network traffic simulation. Cascade effects of some attacks can also be simulated without a real attack if relevant for the current education. Attacks and effects of attacks shall be planned beforehand as part of the exercise scenario (explained later).

3.1.6. Organisations' infrastructures. *Cyber Arena shall include varied organisation environments*. As in the real cyber domain, in addition to the Internet there is also an organisation environment connected to global network infrastructure. Those simulated organisation environments shall include both Information Technology (IT) and Operational Technology (OT) systems as well as interconnections of IT and OT systems and operations. In many cases it will be beneficial to execute two or more organisations in the same training or exercise in order to express interdependences between the organisations at the process and information system level . Good examples of that are an electricity company or an Internet Service Provider (ISP); if there is a cyber attack against those, it will most probably also affect the infrastructure of other organisations. The above-mentioned also illustrates real life interdependencies in organisations, networks and / or ecosystems.

3.1.7. Collaboration. *Cyber Arena shall have the capability for collaboration and co-operation with other training platforms*. According to collaborative learning theory [30], enabling collaboration between the students creates a better opportunity for learning. Students' collaboration enables collegial learning and problem solving. The cyber environment as a working context is very broad. Thus, areas of expertise are bound, which forcesbetween the organisations real-life experts into collegial problem-solving. This is why teamwork is one of the key elements of the cyber security exercise. Additionally, if there is lack of some technical capability of Cyber Arena, it can be achieved by interconnection and co-operation with other technical training platforms.

3.1.8. Planning, executing, monitoring and analysing. *Cyber Arena shall be able to provide authentic activities with real-life scenarios*. The pedagogical goals of the exercise must be taken into account at all stages of the exercise [31]. In order to accomplish this, the Cyber Arena shall have exercise planning, execution, monitoring and analysing capabilities and tools. Via this capability the exercise and the scenarios can be planned and executed but also instructors can evaluate training audience/students' performance assessment and allow training audience/students to evaluate their performance after the exercise. This enables reflection, which is one of the key elements of learning.

4. Conclusion

In this paper the concept Cyber Arena (CA) is introduced and discussed. First, the classical cyber range concept is introduced with the examples of extremely heterogeneous definitions with the term cyber range. Because of the unexpected dependencies of the systems in the digitalised cyber domain and kinetic domain, more complex training infrastructures are required to support training, exercising and learning in complex environments. Especially when it comes to educational activities where a degree program is provided, the program should have a Cyber Arena type of facility in use. If the training and exercises are carried out in a traditional laboratory environments or in limited range environments, the core know how elements of the cyber domain cannot be realised and combined. Thus the key element of technical complexity and the interdependences between the elements will not be involved in the education program.

The pedagogical aspects are introduced for proving the need for the Cyber Arena concept and the Cyber Arena concept is introduced with its high-level requirements. As the result of the paper, it is recommended to use the term Cyber Arena when discussing state-of-the-art modern and complex cyber security exercise platforms. Term cyber range shall be used when discussing classical limited platforms.

As for future research, more specified technical requirements can be developed and state-of-the-art trainings and exercises implemented.

Acknowledgment

This research is funded by *Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)* - project of the Horizon 2020 SU-ICT-03-2018 program.

References

[1] Secretariat of the Security Committee, “Finland’s Cyber security Strategy, Government Resolution 3.10.2019,” Oct. 2019. [Online]. Available: https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf

[2] European Comission, “Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace,” Feb. 2013. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN

[3] P. Nevavuori and T. Kokkonen, “Requirements for training and evaluation dataset of network and host intrusion detection system,” in *New Knowledge in Information Systems and Technologies*, Á. Rocha, H. Adeli, L. P. Reis, and S. Costanzo, Eds. Cham: Springer International Publishing, 2019, pp. 534–546.

[4] National Institute of Standards and Technology NIST, “Cyber Ranges,” https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, Accessed: 13 January 2020.

[5] B. Ferguson, A. Tall, and D. Olsen, “National cyber range overview,” in *2014 IEEE Military Communications Conference*, Oct 2014, pp. 123–128.

[6] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, and X. Cui, “A real-time correlation of host-level events in cyber range service for smart campus,” *IEEE Access*, vol. 6, pp. 35 355–35 364, 2018.

[7] V. E. Urias, W. M. S. Stout, B. Van Leeuwen, and H. Lin, “Cyber range infrastructure limitations and needs of tomorrow: A position paper,” in *2018 International Carnahan Conference on Security Technology (ICCST)*, Oct 2018, pp. 1–5.

[8] M. Yamin, B. Katt, and V. Gkioulos, “Cyber ranges and security testbeds: Scenarios, functions, tools and architecture,” *Computers & Security*, vol. 88, p. 101636, 10 2019.

[9] H. Winter, “System security assessment using a cyber range,” in *7th IET International Conference on System Safety, incorporating the Cyber Security Conference 2012*, Oct 2012, pp. 1–5.

[10] Y. He, L. Yan, J. Liu, D. Bai, Z. Chen, X. Yu, D. Gao, and J. Zhu, “Design of information system cyber security range test system for power industry,” in *2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia)*, May 2019, pp. 1024–1028.

[11] Z. Chen, L. Yan, Y. He, D. Bai, X. Liu, and L. Li, “Reflections on the construction of cyber security range in power information system,” in *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Oct 2018, pp. 2093–2097.

[12] G. M. Deckard, “Cybertropolis: breaking the paradigm of cyber-ranges and testbeds,” in *2018 IEEE International Symposium on Technologies for Homeland Security (HST)*, Oct 2018, pp. 1–4.

[13] M. Frank, M. Leitner, and T. Pahi, “Design considerations for cyber security testbeds: A case study on a cyber security testbed for education,” in *2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech)*, Nov 2017, pp. 38–46.

[14] A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, “Exploring game design for cybersecurity training,” in *2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER)*, May 2012, pp. 256–262.

[15] S. Chapman, R. Smith, L. Maglaras, and H. Janicke, “Can a network attack be simulated in an emulated environment for network security training?” *Journal of Sensor and Actuator Networks*, vol. 6, p. 16, 08 2017.

[16] G. Subaşu, L. Roşu, and I. Bădoi, “Modeling and simulation architecture for training in cyber defence education,” in *2017 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, June 2017, pp. 1–4.

[17] H. Liu, W. Han, and Y. jia, “Construction of cyber range network security indication system based on deep learning,” in *2019 IEEE Fourth International Conference on Data Science in Cyberspace (DSC)*, June 2019, pp. 495–502.

[18] L. Pridmore, P. Lardieri, and R. Hollister, “National cyber range (ncr) automated test tools: Implications and application to network-centric support tools,” in *2010 IEEE AUTOTESTCON*, Sep. 2010, pp. 1–4.

[19] T. Debatty and W. Mees, “Building a cyber range for training cyberdefense situation awareness,” in *2019 International Conference on Military Communications and Information Systems (ICMCIS)*, May 2019, pp. 1–6.

[20] European Defence Agency, EDA, “Cyber ranges: Eda’s first ever cyber defence pooling & sharing project launched by 11 member states,” https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, May 2017, Accessed: 13 January 2020.

[21] European Defence Agency, EDA, “Cyber ranges federation project reaches new milestone,” https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone, Sept 2018, Accessed: 13 January 2020.

[22] European Defence Agency, EDA, “Eda cyber ranges federation project showcased at demo exercise in finland,” https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland, Nov 2019, Accessed: 13 January 2020.

[23] S. Nyström, J. Dahlberg, S. Edelbring, H. Hult, and M. Dahlgren, “Debriefing practices in interprofessional simulation with students: A sociomaterial perspective,” *BMC Medical Education*, vol. 16, 12 2016.

[24] S. Bariran, K. Sahari, and B. Yunus, “A novel interactive obe approach in scm pedagogy using beer game simulation theory,” 04 2014.

[25] V. Emin-Martinez and M. Ney, “Supporting Teachers in the Process of Adoption of Game Based Learning Pedagogy,” in *ECGBL 2013 - European Conference on Games Based Learning*, P. Escudeiro and C. V. de Carvalho, Eds. Porto, Portugal: ACPI, Oct. 2013, pp. 156–162. [Online]. Available: https://hal.archives-ouvertes.fr/hal-00872282

[26] J. Herrington and R. Oliver, "An instructional design framework for authentic learning environments," *Educational Technology Research and Development*, vol. 48, no. 3, pp. 23–48, Sep 2000. [Online]. Available: https://doi.org/10.1007/BF02319856

[27] J. Herrington, "Authentic e-learning in higher education: Design principles for authentic learning environments and tasks," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*. Association for the Advancement of Computing in Education (AACE), 2006, pp. 3164–3173.

[28] A. Collins, "Cognitive apprenticeship and instructional technology. technical report." 1988. [Online]. Available: https://files.eric.ed.gov/fulltext/ED331465.pdf

[29] European Cyber Security Organisation, ECSO, "Understanding Cyber Ranges," https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf, March 2020, Accessed: 6 April 2020.

[30] T. Panitz, "Collaborative versus cooperative learning: A comparison of the two concepts which will help us understand the underlying nature of interactive learning." 1999. [Online]. Available: https://files.eric.ed.gov/fulltext/ED448443.pdf

[31] M. Karjalainen, T. Kokkonen, and S. Puuska, "Pedagogical aspects of cyber security exercises," in *2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE, 2019, pp. 103–108.

V

REVIEW OF PEDAGOGICAL PRINCIPLES OF CYBER SECURITY EXERCISES

by

Mika Karjalainen & Tero Kokkonen, 2020

Advances in Science, Technology and Engineering Systems Journal,
5(5), 592-600

DOI: 10.25046/aj050572

Advances in Science, Technology and Engineering Systems Journal
Vol. ?, No. ?, XXX-YYY (2020)
www.astesj.com
Special Issue on Multidisciplinary Innovation in Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Review of Pedagogical Principles of Cyber Security Exercises

Mika Karjalainen[*], Tero Kokkonen[*]

Institute of Information Technology, JAMK University of Applied Sciences, 40100, Jyväskylä, Finland

ARTICLE INFO

Article history:
Received:
Accepted:
Online:

Keywords:
Cyber Security Exercise
Expert Performance
Simulation Pedagogy

ABSTRACT

Modern digitalized cyber domains are extremely complex ensemble. Cyber attacks or incidents against system may affect capricious effects for another system or even for physical devices. For understanding and training to encounter those effects requires an effective and complex simulation capability. Cyber Security Exercises are an effective expedient for training and learning measures and operations with their outcomes in that complex cyber domain. Learning in cyber security exercises is relevant for different level actors in organisation hierarchy. Technical experts are able to train the technical capabilities whereas decision makers are able to train the decision-making capabilities under hectic cyber incident. In this paper, the pedagogical aspects of cyber security exercises are discussed in accordance with the law of the lifecycle of the cyber security exercise: planning phase, implementation phase, and feedback phase.

1 Introduction

This research is an extension of work originally presented in 2019 workshop on Cyber Range Technologies and Applications (CACOE 2019) organized in conjunction with 2019 IEEE European Symposium on Security and Privacy (EuroS&P 2019) [1]. This research is expanded from the original as follows: discussion about pedagogical theories and cyber-arena concept for complex environment simulation with the more detailed extended analysis of pedagogical aspects of the cyber security exercises and assessment of the exercise target audience.

Global digitalisation and networked systems have raised new threats. Modern digitalised cyber domains are extremely complex and forms incalculable reliance. That change in digital environment has reflected to the requirements of training and education. Traditionally, exercises are used in a military context to gain better performance for certain tasks. In the cyber domain and especially in the context of cyber resilience, the most valuable assets are personal skills. Those skills are trained efficiently with cyber security exercises.

Cyber security strategy of Finland [2] states that in the critical cyber competence areas, the high level of required training is confirmed by both national and international exercises. The significance of cyber security exercises is also observed in the cyber strategy of the United States of America [3] and the cyber security strategy of the European Union [4]. In addition, cyber security exercises are recognized as an important part of personnel training in commercial organisations, especially in the critical infrastructure organisations, for example, electricity companies [5]. There are several different cyber security exercises conducted globally, for example, the report [6] consists of a dataset of more than 200 cyber security exercises and the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) highlights several exercises they organise or contribute [7].

There exist frameworks categorizing the required skills of personnel in organisations . National Institute of Standards and Technology (NIST) has published document called National Initiative for Cyber security Education (NICE) Cyber security Workforce Framework (NICE Framework) as a reference structure that designates the complex essence of the knowledge, skills, and abilities (KSAs) required in the different roles and tasks of the work within cyber security [8, 9]. There are also frameworks for curricula of education: Computing Curricula 2020 (CC2020) forms a guideline for academic degree programs in computing) [10]. When discussing cyber security, the CC2020 refer to the Cyber security Curricula 2017 (CSEC2017) that form curriculum guidelines for degree programs in cyber security [11].

Simulations have been widely used for study experts [12]. Education in the engineering sciences relies heavily on hands-on training, i.e. applying learned phenomena in practice. In that sense, different learning environments, simulators and test-beds have a remarkable role in the engineering education. When discussing cyber security exercises, the extremely important component is the exercise platform that simulates the cyber domain. Traditionally that kind of platform is called cyber range. Cyber range is executed as a technical platform for exercises that mimic the required networks and systems. As exercise platform, a cyber range, is required

[*] Corresponding Authors: Mika Karjalainen, mika.karjalainen@jamk.fi and Tero Kokkonen, tero.kokkonen@jamk.fi

https://dx.doi.org/10.25046/aj??????

to be closed and totally controlled to allow risk free usage of real attacks and intrusions [13, 14, 15]. The term cyber range originates from the similarity of the kinetic ranges with potential to improve competence or capability with weapons, operations, tactics and techniques [16]. As stated in [17], there exist several diverse cyber ranges globally that vary from enormous virtual-Internets to simple laboratory based test-beds. Because the spectrum of cyber ranges is so multifarious, authors of [17] introduced the concept of Cyber Arena for the simulation of realistic complex cyber-physical domain with unexpected dependencies between networks and systems.

JYVSECTEC (Jyväskylä Security Technology) is JAMK University of Applied Sciences Institute of Information Technology based cyber security focused research, development and training center that offers information and cyber security services [18]. JYVSECTEC has extensive experience for organising cyber security exercises for both national security authorities and private companies of critical infrastructure. Since 2013, Finland's national cyber security exercise has been organised annually by JYVSECTEC [19]. JYVSECTEC has also been Finland's representative in the Cyber Defence Pooling & Sharing Project of European Defence Agency (EDA) [20, 21, 22].

JAMK University of Applied Sciences has organised several different cyber security exercises. During those exercises, more than 1,500 experts have been involved in those learning experiments. In addition, there is an annual course of cyber security exercise for the cyber security students of bachelor's and master's programs of JAMK University of Applied Sciences. The data for this research of multiple-case design originates from observations, notes and questionnaires collected from the numerous cyber security exercises organised by JAMK University of Applied Sciences. The focus of this research is to characterize pedagogical principles of cyber security exercises as the educational framework for understanding the complex and interdependent cyber domain in the individual or organisational level.

Albeit, the importance of the cyber security exercises is widely recognized, there is a deficiency in the research of pedagogical aspects, especially in the viewpoint of competence development. In high level, cyber security exercise is a three-phase process consisting of different components of exercise life-cycle: planning phase, implementation phase and feedback phase. Those three phases can be divided into smaller steps of process. This study presents a competence development oriented view on that lifecycle of cyber security exercises. As part of that competence development oriented view, those three different components of exercise life-cycle are explored with the perspective of learning outcomes.

2 Cyber Security Exercises and the Pedagogical Principles

In recent years, cyber security exercises have established their position as a tool for developing the skills of cyber security professionals and as an operating environment for teaching. As business environments and the using of ICT in business have evolved, they have also become more complex at the same time. Consequently, the requirements for teaching environments have also changed.

In order to be able to teach skills that meet the needs of working life, it is necessary to understand the needs and be able to teach them in such a way that teaching builds skills that are needed in working life [23]. According to Ericsson's deliberated practices (DP) theory, the development of specialist skills must take into account the need to set well-defined learning objectives for students and the need to take into account the level of students' existing skills [24]. According to the deliberated practice theory, students do not benefit from the training if the tasks are at a level that they can perform routinely or if the goal setting of competence development has not been done with sufficient accuracy to mirror the student's level of competence.

Modern ICT teaching must therefore be able to mirror the changes in the operating environment to the change in competence requirements. When a modern cyber range is used in a cyber security exercise, the aim must be to make the operating environment as realistic as possible. The comprehensiveness and complexity of the teaching environment places demands on the student's level of competence. Thus, if cyber security training is used as a pedagogical tool for competence development, it should be noted that according to the Miller pyramid, the student's level of competence should be at the top of the pyramid [25]. This argument is supported by the andragogy, known as a theory of adult learning. According to andragogy theory an adult as a learner is often motivated, capable of self-direction and reflection on one's own existing competence [26]. Thus, for the adult learner learning experiment should be able to cause cognitive dissonance that allows the learner to update existing knowledge with new knowledge created in the learning event [27]. It must be possible to build a path of competence development, where in accordance with the constructive methodology, the student's developing competence enables the student to achieve new levels of competence through developing cognitive abilities [28]. Constructive methodology identifies problem-based learning as one of the key learning methods, in which the student develops his or her own skills by solving problems that lead to the learner's new knowledge [29].

The cyber security exercise can be seen as a complex problem field where the student solves the problems ahead and thus generates new knowledge for himself. This theory is supported also by experiential learning theory [30]. A key element in cyber security practice is working as a member of a team. This models real-life work where a person acts as part of, for example, a security operation team (SOC). In the exercise, all individuals are placed as a member of Teams (Blue Team) whose job is to defend and sustain the business in the operating environment assigned to them. The student can also act as part of a red team functionality that simulates threat activities. This role is to train, for example, the skills required for penetration testing. In the exercise, learners act in the role assigned to them, and communicate as part of a team of events that they perceive in their own operating environment. Thus, students share knowledge, solve problems and build new knowledge collectively.

To sum up, the cyber security exercise combines several pedagogical theories. The pedagogical framework of the cyber security exercises is shown in Figure 1. The exercise is also demanding from the point of view of pedagogical implementation and often requires a significant investment in pre-exercise planning, where the operating environment is constructed so that the required technical elements can be modeled and operational functionalities are designed so that pedagogical objectives can be achieved.

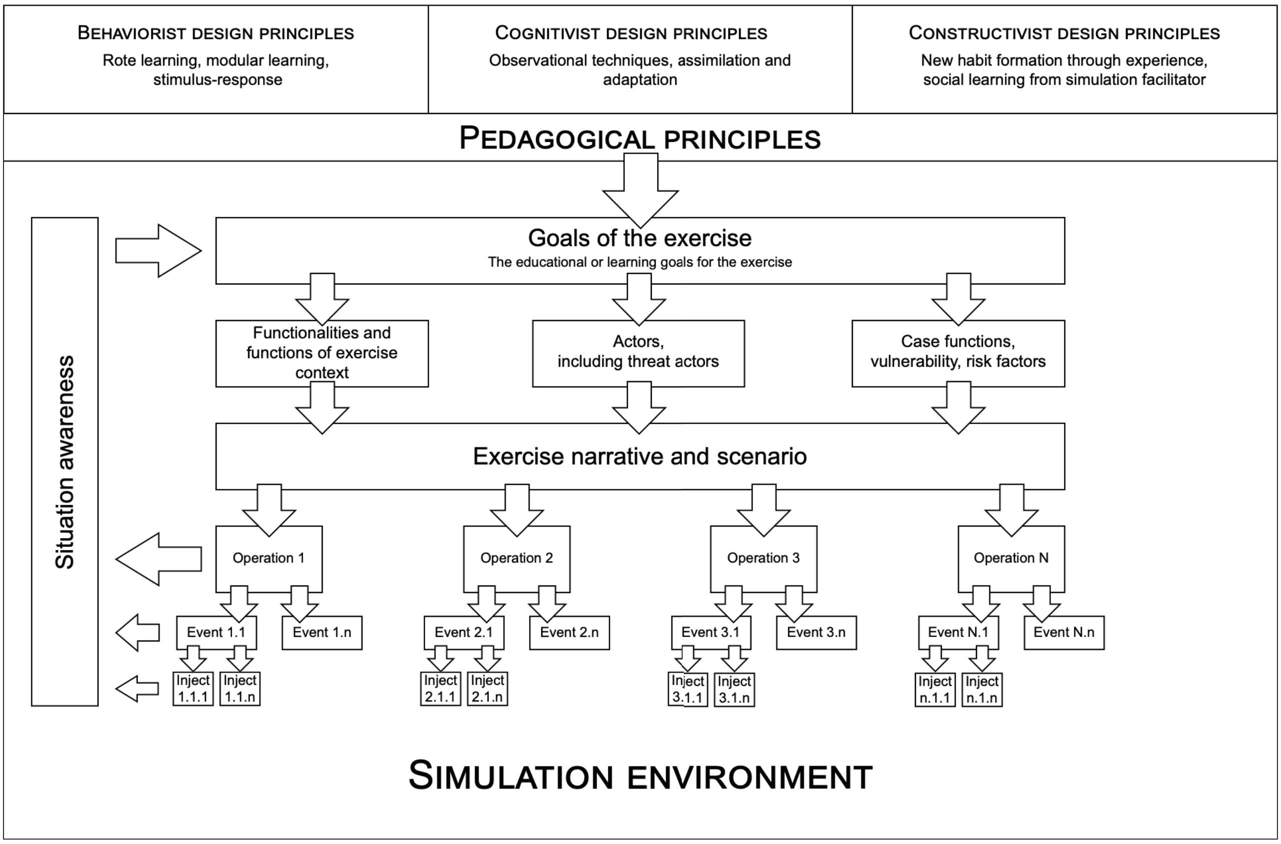

BEHAVIORIST DESIGN PRINCIPLES
Rote learning, modular learning, stimulus-response
COGNITIVIST DESIGN PRINCIPLES
Observational techniques, assimilation and adaptation
CONSTRUCTIVIST DESIGN PRINCIPLES
New habit formation through experience, social learning from simulation facilitator
PEDAGOGICAL PRINCIPLES
Situation awareness
Goals of the exercise
The educational or learning goals for the exercise
Functionalities and functions of exercise context
Actors, including threat actors
Case functions, vulnerability, risk factors
Exercise narrative and scenario
Operation 1
Operation 2
Operation 3
Operation N
Event 1.1
Event 1.n
Event 2.1
Event 2.n
Event 3.1
Event 3.n
Event N.1
Event N.n
Inject 1.1.1
Inject 1.1.n
Inject 2.1.1
Inject 2.1.n
Inject 3.1.1
Inject 3.1.n
Inject n.1.1
Inject n.1.n
SIMULATION ENVIRONMENT

Figure 1: Pedagogical framework of the cyber security exercises [1]

2.1 Cyber Arena

According to complexity thinking, it should be possible to form an understanding of the functionality or entity under investigation as a whole, which is more than the sum of its parts [31]. The operating environment of cyber security can be seen as a complex entity consisting of different parts that interact with each other. Interaction takes place at different levels, such as in the technical operating environment, at the level of activities and processes, and as human interaction. The interconnection between different parts of the operating environment is partly defined and partly undefined. The key elements of complexity thinking are the recognition of the unpredictability of the environment, the difficulty of predicting cause consequences, and the self-organisation of the operating environment [32]. It is thus a matter of utilizing complexity thinking in accordance with the neo-reductionist school to model and simulate the subordination laws of the research object [33].

When the above is applied to the cyber environment, it is noteworthy to recognize the difficulties of applying traditional legislation, technological incompatibilities and the very rapid technical renewal of the environment. Thus, the student should be able to develop an understanding of unpredictability of the environment, unpredictable cause-and-effect relationships, and the risks of misuse of the technological element. In order for this entity to be embodied as part of cyber security education, a sufficiently realistic learning environment should be in place, such as Cyber Arena the overall high-level presentation of which is shown in Figure 2. It can be seen from the figure that the environment extensively models the cyber security domain. In order to be able to implement sufficient realism and the understanding of complexity, the teaching environment should model key functions and entities, as well as the interdependencies between the functions and or entities. In accordance with the authentic learning environment theory [34], the environment implements an operating environment in which the skills and competencies learned in cyber security practice will be applied.

3 Exercise Life-cycle

There are different definitions for the phases of cyber security exercise life-cycle. Wilhelmson and Svensson introduce three phases; planning, implementing and processing feedback, which are divided into into ten steps (exercise preparations, the master plan, the mission statement, exercise planning, practical preparations, implementation, evaluation, feedback, reporting, and the after action review) [35]. Consistently, MITRE describes three stages (Exercise Planning, Exercise Execution and Post Exercise) [36]. Vykopal et al. defines five stages for exercise; preparation, dry run, execution, evaluation, and repetition [37]. The Homeland Security Exercise and Evaluation Program (HSEEP) that provides a set of foundational concepts for exercise programs defines the management cycle with four stages: exercise design and development, exercise conduct, ex-

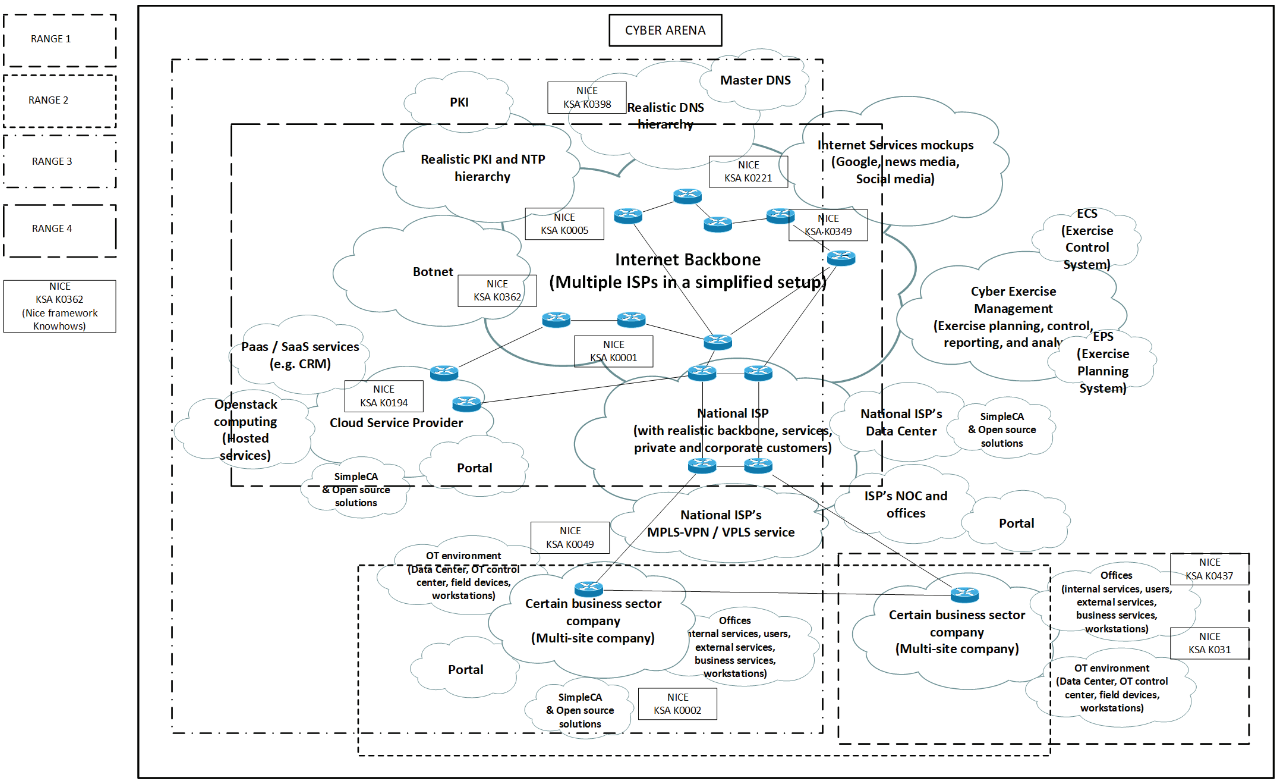

RANGE 1
RANGE 2
RANGE 3
RANGE 4
NICE KSA K0362 (Nice framework Knowhows)
CYBER ARENA
PKI
NICE KSA K0398
Realistic DNS hierarchy
Master DNS
Realistic PKI and NTP hierarchy
NICE KSA K0221
Internet Services mockups (Google, news media, Social media)
NICE KSA K0005
NICE KSA-K0349
ECS (Exercise Control System)
Botnet
NICE KSA K0362
Internet Backbone (Multiple ISPs in a simplified setup)
Cyber Exercise Management (Exercise planning, control, reporting, and analy
EPS (Exercise Planning System)
Paas / SaaS services (e.g. CRM)
NICE KSA K0001
NICE KSA K0194
Openstack computing (Hosted services)
Cloud Service Provider
National ISP (with realistic backbone, services, private and corporate customers)
National ISP's Data Center
SimpleCA & Open source solutions
Portal
SimpleCA & Open source solutions
ISP's NOC and offices
Portal
NICE KSA K0049
National ISP's MPLS-VPN / VPLS service
OT environment (Data Center, OT control center, field devices, workstations)
Certain business sector company (Multi-site company)
Offices (internal services, users, external services, business services, workstations)
Portal
SimpleCA & Open source solutions
NICE KSA K0002
Certain business sector company (Multi-site company)
Offices (internal services, users, external services, business services, workstations)
NICE KSA K0437
NICE KSA K031
OT environment (Data Center, OT control center, field devices, workstations)

Figure 2: Comprehensive Cyber Arena [17]

ercise evaluation, and improvement planning [38]. As an integration of different definitions and a viewpoint for pedagogical aspects of this research the following three phases are selected *(i) planning phase, (ii) implementation phase, and (iii) feedback phase*. The extended view for pedagogical aspects of the cyber security exercises is shown in Figure 3. It illustrates whole process from planning phase to the implementation of the exercise.

3.1 Planning Phase

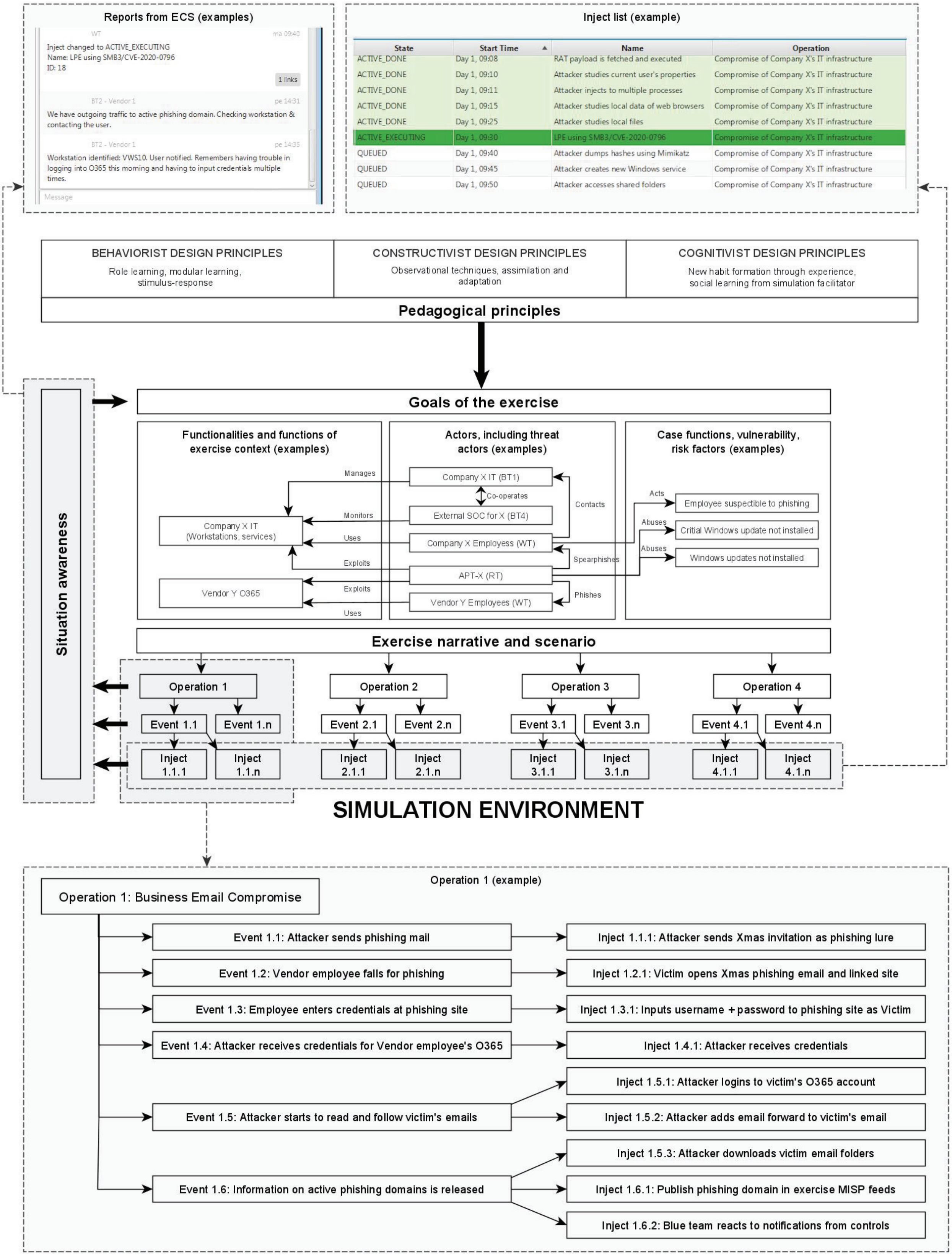
The first step of exercise life-cycle is the planning-phase. It is an extremely critical phase, because it determines the effectiveness of the whole exercise. From the viewpoint of competence development, the content of the exercise e.g. scenario, actors, and events shall be fitted to the requirements of the exercise target audience.

Based on the required learning outcomes and the target organisation, exercise parameters are derived including simulated operational environment of scenario for example technical functionalities, threat actors, risks and vulnerabilities. That scenario encompasses discrete events and injects of exercise describing the totality of simulated activities. If the scenario created during the planning phase includes obscurities, the exercise including technical environment may not increase the performance of the exercise target audience or organisation. All the elements mentioned supports the achievement of the set learning objectives. The learning objectives can be seen at several levels, the goals can be set from the perspective of organisational competence development, on the other hand, learning objectives can be set from the perspective of individual competence development. When learning goals are set from an organisational perspective, an individuals learning goals should be set so that they put the organisations goals into practice. In Figure 3, the goals of the exercise phase are opened, allowing us to look at an example of what kind of practical sections or tasks in the planning phase should be planned in order to be able to achieve the set goals in the exercise.

3.2 Implementation Phase

There are several differences between the phases of the exercise life-cycle. The most hectic phase is the implementation phase where the exercise target audience is acting in a simulated complex cyber domain under cyber deviation actions (attacks and intrusions). When acting under hectic and stressful cyber deviation circumstances, there is a requirement to maintain the understanding (situation awareness, SA) of the valuable assets' status in cyber domain. According to Endsley [39] *"Situation awareness is the perception of the elements in the environment within a volume of time and space, the comprehension of their meaning, and the projection of their status in the near future"*. The expertise of the individual has a remarkable outcome for the SA [40]. In this context, the term situation awareness refers to both, the understanding of the progress of the operational situation in the exercise, and the understanding of the monitoring and evaluation of the pedagogical objectives of the exercise.

During the exercise, also the decision making has a remarkable role in what incident handling actions shall be done and how to



Reports from ECS (examples)

WT ma 09:40
Inject changed to ACTIVE_EXECUTING
Name: LPE using SMB3/CVE-2020-0796
ID: 18
1 links

BT2 - Vendor 1 pe 14:31
We have outgoing traffic to active phishing domain. Checking workstation & contacting the user.

BT2 - Vendor 1 pe 14:35
Workstation identified: VWS10. User notified. Remembers having trouble in logging into O365 this morning and having to input credentials multiple times.

Message

Inject list (example)

State	Start Time	Name	Operation
ACTIVE_DONE	Day 1, 09:08	RAT payload is fetched and executed	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:10	Attacker studies current user's properties	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:11	Attacker injects to multiple processes	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:15	Attacker studies local data of web browsers	Compromise of Company X's IT infrastructure
ACTIVE_DONE	Day 1, 09:25	Attacker studies local files	Compromise of Company X's IT infrastructure
ACTIVE_EXECUTING	Day 1, 09:30	LPE using SMB3/CVE-2020-0796	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:40	Attacker dumps hashes using Mimikatz	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:45	Attacker creates new Windows service	Compromise of Company X's IT infrastructure
QUEUED	Day 1, 09:50	Attacker accesses shared folders	Compromise of Company X's IT infrastructure

BEHAVIORIST DESIGN PRINCIPLES
Role learning, modular learning, stimulus-response
CONSTRUCTIVIST DESIGN PRINCIPLES
Observational techniques, assimilation and adaptation
COGNITIVIST DESIGN PRINCIPLES
New habit formation through experience, social learning from simulation facilitator
Pedagogical principles
Situation awareness
Goals of the exercise
Functionalities and functions of exercise context (examples)
Actors, including threat actors (examples)
Case functions, vulnerability, risk factors (examples)
Manages
Company X IT (BT1)
Co-operates
Contacts
Monitors
External SOC for X (BT4)
Company X IT (Workstations, services)
Uses
Company X Employess (WT)
Spearphishes
Exploits
APT-X (RT)
Exploits
Vendor Y O365
Phishes
Vendor Y Employees (WT)
Uses
Acts
Employee suspectible to phishing
Abuses
Critial Windows update not installed
Abuses
Windows updates not installed
Exercise narrative and scenario
Operation 1
Operation 2
Operation 3
Operation 4
Event 1.1
Event 1.n
Event 2.1
Event 2.n
Event 3.1
Event 3.n
Event 4.1
Event 4.n
Inject 1.1.1
Inject 1.1.n
Inject 2.1.1
Inject 2.1.n
Inject 3.1.1
Inject 3.1.n
Inject 4.1.1
Inject 4.1.n
SIMULATION ENVIRONMENT
Operation 1 (example)
Operation 1: Business Email Compromise
Event 1.1: Attacker sends phishing mail
Inject 1.1.1: Attacker sends Xmas invitation as phishing lure
Event 1.2: Vendor employee falls for phishing
Inject 1.2.1: Victim opens Xmas phishing email and linked site
Event 1.3: Employee enters credentials at phishing site
Inject 1.3.1: Inputs username + password to phishing site as Victim
Event 1.4: Attacker receives credentials for Vendor employee's O365
Inject 1.4.1: Attacker receives credentials
Inject 1.5.1: Attacker logins to victim's O365 account
Event 1.5: Attacker starts to read and follow victim's emails
Inject 1.5.2: Attacker adds email forward to victim's email
Inject 1.5.3: Attacker downloads victim email folders
Event 1.6: Information on active phishing domains is released
Inject 1.6.1: Publish phishing domain in exercise MISP feeds
Inject 1.6.2: Blue team reacts to notifications from controls

Figure 3: Detailed pedagogical framework of the cyber security exercises

categorize order of the required actions. Mostly, those decisions are based on SA as comprehension on two models of decision making cycle; Gartner's Adaptive Security Architecture (Predict-Prevent-Detect-Respond) [41] and OODA-loop (Observation-Orientation-Decision-Action) [42, 43].

Figure 3, illustrates that the operation line according to the exercise scenario, is opened to illustrate the practical actions of one operation performed during the exercise. The operation includes a series of events that are divided into injects with which the exercise is practically carried forward according to a planned scenario. An inject list has also been opened in the figure to show how in the practice the exercise proceeds with injects. The exercise management team (white team, WT) can use the information obtained through information systems to assess the situation, but it is often also necessary to monitor visually and interview students. This will ensure that the exercise proceeds as planned and that the set learning objectives can be achieved. If the WT notices that students are taking actions that are not realistic or the focus of the exercise begins to shift from the set goal, the WT should guide the course of the exercise. This can be done through information system injections or verbally by instructing students.

3.3 Feedback Phase

From the perspective of the development of an individual's competence, the feedback phase is the most important part of the exercise. Scheduling the feedback phase should be planned carefully with too long an interval of exercise and feedback may cause a decrease in learning intensity for the individual. The emotions and experiences raised by the exercise are alleviated and learning outcomes may suffer as a result. In the feedback phase, the pedagogical goals of the exercise are recalled and the events of the exercise are reflected against them by reviewing all operations performed and related events and injects in the exercise. This happens so that all operations performed in the exercise, related events and injects are reviewed. By doing so, the student can reflect the experience they have had during the exercise and thus deepen their own learning. It is also important to tie individual events through operations into an exercise scenario. This allows the student to increase the understanding of the bigger picture, for example, the threat actors´ motive and the tools used for the attack. This is important and enables in the future the exercise event to be reflected in real situations of working life.

It is a good to set aside time for the feedback session so that the interaction between students and teachers can be enabled as widely as possible. Normally, each defensive team (blue team, BT) has the opportunity to open up their own observations and experiences in this section. This enables collegial and collaboratively learning. The offensive team (RT) also goes through its own operations, thus allowing BT to reflect its own observations in relation to the operations that took place.

4 Assessing Performance and Results

The Kirkpatrick four-level assessment framework can be used for the assessment of the exercise. Kirkpatrick divides assessment into four levels: (i) reaction, (ii) learning, (iii) behaviour, and (iv) results [44]. The Kirkpatrick framework is useful in assessing a larger entity such as an organisation or team, but it can also be used for the individual experience of learning in exercise. In the Kirkpatrick framework, the goals for the development of individual competence are set at level one and two. At level one the reactions caused by the exercise are assessed. At level two, the learning that has achieved by the individual is assessed. Kirkpatrick et al. recommends the use of control groups and tests for assessing the learning. The goals set for organisational competence development utilize the Kirkpatrick assessment model´s, level three, which assesses the change in individual behaviour through the achieved learning outcomes, and level four which assesses the effects and implementation of advanced competence on organisational performance. Kirkpatrick model is a widely used evaluation model, the study [45] presents a framework for competence development and assessment in hybrid cyber security exercises, and the authors of [46] introduce one adoption of the Kirkpatrick Model.

Other methods for evaluating exercise can also be used, the authors of [47] have monitored communication during the cyber security exercise for understanding the behaviour of the exercise target audience. Their conclusion is that communication monitoring can be used as a resource in measuring the performance during the cyber security exercise.

When focusing on assessing the learning of an individual who has participated in the exercise, Brown and Pickford [48], have created a model that looks at the assessment of learning event as a whole. Brown and Pickford divide the assessment into the following subsections the significance and implementation of these sections should be planned in advance: why, what, how, who, when.

Why- why the assessment is made? What is the purpose of assessment in this particular learning event? In the context of a cyber security exercise, the aim of assessment is in some respects to control the individual's performance, facilitate the student's adaptation to the exercise, be able to assess the student's motivation, measure the competence, skills and know-how and to provide the student information about mistakes and inappropriate practices.

What- what are we assessing? In a cyber security exercise the processes of work, individual performance and success of team work can be assessed. In the exercise, the assessment should be performed at all stages of its life cycle.

How- how are we assessing? As discussed, Figure 3 illustrates the role of the situation awareness and all the inputs where the information for assessing will be collected. So, part of the information for the assessment can be collected via information systems and the reports from the BT that they are delivering to exercise control system. In addition to this, the teacher must monitor classroom activities. In this way, information can be obtained, for example, about an individual's performance in a specific role as part of a team. Visual observation can also provide information about the team's internal activities and role support and its possible functioning.

Who- who is suitable for making the assessment? In the exercise, students often work as a part of a team throughout the exercise. This provides an opportunity to implement the evaluation as a peer review, whereby the internal functionalities and inclusions of the team become more clearly assessed. In education leading to a degree, students are also often asked to have a learning diary in which the student can make a self-assessment of the exercise throughout its life cycle. The role of teachers in the assessment may therefore be more aggregate.

When- when should assessment take place? In the cyber security exercise the assessment needs to be done in all phases of exercise. This is because the assessment plays a very important role as a function of guiding learning. The importance of formative or guiding assessment in cyber security exercises is emphasized. The theory of formative evaluation has been built specifically by Scriven [49]. According to Scriven, the concept of formative assessment became conceptualized. Formative assessment emphasizes that assessment should take place at all stages of the teaching and learning, and not just at the end. Several studies verify that learning outcomes are significantly improved when formative assessment that guides learning is included in the assessment as well as summative assessment. Thomas et. al [50] and Leahy et. al [51] have stated that learning outcomes improve when assessment includes formative assessment that guides learning in addition to the assessment learned skills.

Formative assessment emphasizes the importance of feedback. According to Hattie [52], the purpose of the feedback can be divided into three sections: *Feed up, feed back* and *feed forward* sections. The feed up gives the learner an answer to the question of where he or she is going. The purpose of feed up feedback is to continuously clarify and specify the learning objectives. Feed up feedback also aims to engage and motivate the learner to pursue to the set goals. A feed back, tells to the learner where he or she is at the moment. The feed back feedback is used to provide the student the information on how he or she has progressed in relation to the set learning objectives. In order to give exact feedback on the learner's position, the learning objectives must be precisely defined, also so that the prerequisites for progressive learning are perceptible and acceptable. Feed forward feedback, tells the learner what he or she should do next. In practice, guidance can be sought, for example, through questions that broaden the student's understanding, or with advice and tips on, for example, new ways for approaching to the set goals.

According to Hattie, each feedback question works on four levels: level of the task, level of process, level of self-regulation and level of person. The level of the task, i.e. how well the learner understands the set tasks and how he or she performs them. In practice, for example, feedback indicates whether an individual task has been solved correctly or incorrectly. Feedback should also be directed to correcting any malfunctions or performing the task correctly. Level of process indicates the process required to understand and perform a given task in the context of a cyber exercise, for example, what kind of operation is needed to bring an into the exercise so that the student learns the methods and technology used for a phishing campaigns. Level of self-regulation guides the learner to self-assessment and self-direction of action. At this level, feedback can also be used to guide the learner's motivation and adaptation to the teaching environment used. The level of the person includes assessments of the learner. This section often contains elements for assessing and providing feedback on a learners personality traits. In a cyber exercise, guidance can be given, for example, on a persons participation and activity as part of a team, what is a key part of a persons performance in the exercise.

The purpose of the feedback is to reduce the gap between existing competence and the target competence. Due to the complexity and scope of the cyber security exercise, special attention should be paid to the continuous feedback throughout the exercise life cycle.

5 Conclusion

There are elements in the cyber security operating environment in line with complexity thinking, however, it is a philosophical question of whether the cyber security environment is ultimately a complex entity. There is complexity in the operating environment. According to the definition of complexity, the phenomena are intertwined and the whole cannot be understood by disassembling the whole into parts and looking at the parts one by one. Unlike complex entities, the cyber operation environment can be controlled, although there may also be self-directed elements in the operation environment. When implementing cyber security education, the complexity of the operating environment should be taken into account. Therefore, the teaching environment should be a Cyber Arena style operating environment mimicking realistic operative cyber domain. In the Cyber Arena, several functional entities are combined forming an ensemble with complex cause-and-effect relationships manifested. Pedagogically, however, the constructive construction of competence development must be taken into account, in which case teaching starts from the parts or details of the operating environment and culminates the teaching for understanding the whole environment, including the interdependences of different entities.

As presented, the pedagogical objectives of the exercise should be taken into account at all stages of the life cycle. In the planning phase, goals are set for competence development. In education leading to a degree, the objectives are defined in the curriculum. In the exercise for the other target audience, the goals of competence development should be defined together with the representatives of the organisation. In this way, the objectives of the exercise are adapted to the current maturity and operations of the organisation. In the implementation phase, the realization of the goals must be monitored and, if necessary, the focus of the exercise must be directed towards the set goals. In the feedback phase, participants in the exercise are given the opportunity to interact through the exercise, in which the operations performed in the exercise are opened in detail. To support post-practice learning, it is also important to provide material to be distributed that allows students to return to the details of the exercise afterwards.

Generally accepted content frameworks, such as the NICE framework,can be used to design the content's learning objectives. This makes it possible to set structured teaching goals, through which the exercise scenario can be constructed in such a way that the technical functions do not remain separate events without causal relationships. The student who has done this is are able to form an entity from the exercise, at the latest at the feedback stage, through which he or she can learn about the effectiveness of the sub-entities of the operating environment as a whole.

Exercise evaluation is a challenging whole consisting of evaluating an individual, as well as evaluating the performance of an organisation or part of it. In order for assessment to serve the set competence development goals as well as possible, formative assessment that guides learning should be used where possible. In this way, the evaluation of the activities serves as a guiding element of the exercise, helping to ensure that the set learning objectives are achieved. With regard to formative assessment, the importance of feedback is emphasized. It should be possible to deliver it at all stages of the exercise life cycle. Feedback should take into account interactivity and, where possible, make use of peer feedback from learners.

Future research should build on the understanding of the pedagogical requirements of cyber security exercise in relation to the teaching environment and individual learning gained in this and other studies and move towards assessing the development of organisational competence in cyber security exercise.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research is funded by the *Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)* project of the Horizon 2020 SU-ICT-03-2018 program.

References

[1] M. Karjalainen, T. Kokkonen, S. Puuska, "Pedagogical Aspects of Cyber Security Exercises," in "2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&p)," 103–108, 2019, http://dx.doi.org/10.1109/EuroSPW.2019.00018.

[2] Secretariat of the Security Committee, "Finland's Cyber security Strategy, Government Resolution 3.10.2019," https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf, 2019.

[3] The White House, signed by President Donald J. Trump, "National Cyber Strategy of the United States of America," https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf, 2018.

[4] European Comission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace," https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52013JC0001&from=EN, 2013.

[5] FINGRID magazine, "Cyber security is ensured with genuine exercises," https://www.fingridlehti.fi/en/cyber-security-ensured-genuine-exercises/, 2017, Accessed: 12 May 2020.

[6] B. Uckan Färnman, M. Koraeus, S. Backman, "The 2015 Report on National and International Cyber Security Exercises : Survey, Analysis and Recommendations," Technical report, Swedish Defence University, CRISMART (National Center for Crisis Management Research and Training), 2015, http://dx.doi.org/10.2824/627469.

[7] The NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE, "Exercises," https://ccdcoe.org/exercises/, Accessed: 12 May 2020.

[8] K. Saharinen, M. Karjalainen, T. Kokkonen, "A Design Model for a Degree Programme in Cyber Security," in "Proceedings of the 2019 11th International Conference on Education Technology and Computers," ICETC 2019, 3–7, Association for Computing Machinery, New York, NY, USA, 2019, http://dx.doi.org/10.1145/3369255.3369266.

[9] W. Newhouse, S. Keith, B. Scribner, G. Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, 2017, http://dx.doi.org/10.6028/nist.sp.800-181.

[10] Association for Computing Machinery (ACM) and IEEE Computer Society (IEEE-CS), "Computing Curricula 2020, CC2020, Paradigms for Future Computing Curricula (Draft, Version 36)," https://cc2020.nsparc.msstate.edu/, 2020.

[11] Association for Computing Machinery (ACM) and IEEE Computer Society (IEEE-CS) and Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8), "Cybersecurity Curricula 2017, (CSEC2017), Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (Version 1.0)," https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf, 2017, Accessed: 12 May 2020.

[12] P. Ward, A. M. Williams, P. A. Hancock, Simulation for Performance and Training, 243–262, Cambridge University Press, New York, NY, US, 2006, http://dx.doi.org/10.1017/CBO9780511816796.014, iD: 2006-10094-014.

[13] P. Nevavuori, T. Kokkonen, "Requirements for Training and Evaluation Dataset of Network and Host Intrusion Detection System," in Á. Rocha, H. Adeli, L. P. Reis, S. Costanzo, eds., "New Knowledge in Information Systems and Technologies," 534–546, Springer International Publishing, Cham, 2019.

[14] National Institute of Standards and Technology NIST, "Cyber Ranges," https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf, Accessed: 12 May 2020.

[15] B. Ferguson, A. Tall, D. Olsen, "National Cyber Range Overview," in "2014 IEEE Military Communications Conference," 123–128, 2014, http://dx.doi.org/10.1109/MILCOM.2014.27.

[16] Z. Tian, Y. Cui, L. An, S. Su, X. Yin, L. Yin, X. Cui, "A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus," IEEE Access, **6**, 35355–35364, 2018, http://dx.doi.org/10.1109/ACCESS.2018.2846590.

[17] M. Karjalainen, T. Kokkonen, "Comprehensive Cyber Arena; The Next Generation Cyber Range," in "2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&P)," , 2020.

[18] JAMK University of Applied Sciences, Institute of Information Technology, JYVSECTEC, "Jyväskylä Security Technology," https://www.jyvsectec.fi, Accessed: 12 May 2020.

[19] Ministry of Defence Finland, "Kansallinen kyberturvallisuusharjoitus KYHA18 järjestetään Jyväskylässä, Official Bulletin 11th of May 2018," https://www.defmin.fi/ajankohtaista/tiedotteet/2018?9610_m=9314, 2018, Accessed: 12 May 2020.

[20] European Defence Agency, EDA, "Cyber Ranges: EDA's First Ever Cyber Defence Pooling & Sharing Project Launched By 11 Member States," https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states, 2017, Accessed: 12 May 2020.

[21] European Defence Agency, EDA, "Cyber Ranges Federation Project reaches new milestone," https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone, 2018, Accessed: 12 May 2020.

[22] European Defence Agency, EDA, "EDA Cyber Ranges Federation project showcased at demo exercise in Finland," https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland, 2019, Accessed: 12 May 2020.

[23] H. Collins, R. Evans, A Sociological/Philosophical Perspective on Expertise: The Acquisition of Expertise through Socialization, 21–32, Cambridge Handbooks in Psychology, Cambridge University Press, 2 edition, 2018, http://dx.doi.org/10.1017/9781316480748.002.

[24] K. Anders Ericsson, "Deliberate Practice and Acquisition of Expert Performance: A General Overview," Academic Emergency Medicine, **15**(11), 988–994, 2008, http://dx.doi.org/10.1111/j.1553-2712.2008.00227.x.

[25] G. E. Miller, "The assessment of clinical skills/competence/performance," Academic medicine, **65**(9), S63–7, 1990.

[26] S. B. Merriam, L. L. Bierema, Adult learning: Linking theory and practice, John Wiley & Sons, 2013.

[27] M. S. Knowles, Designs for adult learning: Practical resources, exercises and course outlines from the father of adult learning., Alexandria, Va: American Society for Training & Development, 1995.

[28] S. Lindblom-Ylänne, A. Nevgi, "The effect of pedagogical training and teaching experience on approach to teaching," in "11th EARLI conference, Padua," , 2003.

[29] J. R. Savery, T. M. Duffy, "Problem based learning: An instructional model and its constructivist framework," Educational technology, **35**(5), 31–38, 1995.

[30] D. A. Kolb, R. E. Boyatzis, C. Mainemelis, et al., "Experiential learning theory: Previous research and new directions," Perspectives on thinking, learning, and cognitive styles, **1**(8), 227–247, 2001.

[31] T. Hanén, "Faced with the Unexpected - Leadership in Unexpected and Dynamic Situations: an Interpretation Based on Complexity Theory (Orig: Yllätysten edessä: kompleksisuusteoreettinen tulkinta yllättävien ja dynaamisten tilanteiden johtamisesta)," Ph.D. thesis, National Defence University, 2017, http://urn.fi/URN:ISBN:978-951-25-2870-7.

[32] R. Geyer, S. Rihani, Complexity and public policy: a new approach to twenty-first century politics, policy and society, Routledge, 2010.

[33] K. A. Richardson, "MANAGING COMPLEX ORGANIZATIONS: COMPLEXITY THINKING AND THE SCIENCE AND ART OF MANAGEMENT," Corporate Finance Review, **13**(1), 23–29, 2008, https://search-proquest-com.ezproxy.jyu.fi/docview/198834948?accountid=11774.

[34] J. Herrington, R. Oliver, "An instructional design framework for authentic learning environments," Educational Technology Research and Development, **48**(3), 23–48, 2000, http://dx.doi.org/10.1007/BF02319856.

[35] N. Wilhelmson, T. Svensson, Handbook for planning, running and evaluating information technology and cyber security exercises, The Swedish National Defence College, Center for Asymmetric Threats Studies (CATS), 2014.

[36] J. Kick, "Cyber Exercise Playbook," The MITRE Corporation https://www.mitre.org/sites/default/files/publications/pr_14-3929-cyber-exercise-playbook.pdf, 2014, Accessed: 12 May 2020.

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

[38] The U.S Department of Homeland Security, "Homeland Security Exercise and Evaluation Program (HSEEP)," https://www.fema.gov/media-library-data/1582669862650-94efb02c8373e28cadf57413ef293ac6/Homeland-Security-Exercise-and-Evaluation-Program-Doctrine-2020-Revision-2-2-25.pdf, 2020, Accessed: 12 May 2020.

[39] M. Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," Human Factors, **37**(1), 32–64, 1995, http://dx.doi.org/10.1518/001872095779049543.

[40] M. R. Endsley, Expertise and Situation Awareness, 633–652, Cambridge Handbooks in Psychology, Cambridge University Press, 2006, http://dx.doi.org/10.1017/CBO9780511816796.036.

[41] R. van der Meulen, "Build Adaptive Security Architecture Into Your Organization," https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization/, 2017, accessed: 3 April 2020.

[42] G. L. Rogova, R. Ilin, "Reasoning and Decision Making under Uncertainty and Risk for Situation Management," in "2019 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)," 34–42, 2019, http://dx.doi.org/10.1109/COGSIMA.2019.8724330.

[43] B. Brehmer, "The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control," in "10th International Command and Control Research and Technology Symposium, The Future of C2," , 2005.

[44] D. L. Kirkpatrick, J. D. Kirkpatrick, Evaluating Training Programs, Berrett-Koehler Publishers, Inc., San Francisco, 2006.

[45] A. Brilingaitė, L. Bukauskas, A. Juozapavičius, "A framework for competence development and assessment in hybrid cybersecurity exercises," Computers & Security, **88**, 101607, 2020, http://dx.doi.org/10.1016/j.cose.2019.101607.

[46] A. Ahmad, C. Johnson, "A Cyber Exercise Post Assessment: Adoption of the Kirkpatrick Model," Advances in Information Sciences and Service Sciences (AISS), **7**(2), 2015.

[47] T. Kokkonen, S. Puuska, "Blue Team Communication and Reporting for Enhancing Situational Awareness from White Team Perspective in Cyber Security Exercises," in O. Galinina, S. Andreev, S. Balandin, Y. Koucheryavy, eds., "Internet of Things, Smart Spaces, and Next Generation Networks and Systems," 277–288, Springer International Publishing, Cham, 2018.

[48] S. Brown, R. Pickford, Assessing skills and practice, Routledge, 2006.

[49] M. Scriven, "SOCIAL SCIENCE EDUCATION CONSORTIUM. PUBLICATION 110, THE METHODOLOGY OF EVALUATION." , 1966.

[50] L. Thomas, C. Deaudelin, J. Desjardins, O. Dezutter, "Elementary teachers' formative evaluation practices in an era of curricular reform in Quebec, Canada," Assessment in Education: Principles, Policy & Practice, **18**(4), 381–398, 2011.

[51] S. Leahy, D. Wiliam, "From teachers to schools: scaling up professional development for formative assessment," Assessment and learning, **2**, 49–71, 2012.

[52] J. Hattie, "Teachers Make a Difference, What is the research evidence?" , 2003.

VI

KEY ELEMENTS OF ON-LINE CYBER SECURITY EXERCISE AND SURVEY OF LEARNING DURING THE ON-LINE CYBER SECURITY EXERCISE

by

Mika Karjalainen, Tero Kokkonen & Niko Taari, 2021

Cyber Security: Critical Infrastructure Protection. Springer, Cham. To appear.

Request a copy from author.

VII

A DESIGN MODEL FOR A DEGREE PROGRAMME IN CYBER SECURITY

by

Karo Saharinen, Mika Karjalainen & Tero Kokkonen, 2019

ICETC 2019: Proceedings of the 2019 11th International Conference on Education Technology and Computers (pp. 3–7). ACM, New York.

DOI: 10.1145/3369255.3369266

A Design Model for a Degree Programme in Cyber Security

Karo Saharinen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 410 4415
karo.saharinen@jamk.fi

Mika Karjalainen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 40 574 8012
mika.karjalainen@jamk.fi

Tero Kokkonen
JAMK University of Applied Sciences
Piippukatu 2
40100 Jyväskylä
+358 50 438 5317
tero.kokkonen@jamk.fi

ABSTRACT

The need for skillful cyber security workforce has increased dramatically during the last ten years. The contents of the degree programmmes have not been able to respond to this need adequately and the curriculum contents have not always met the industry's knowledge needs.

In this paper, we describe a model for designing a degree programme in Cyber Security. We establish the guiding frameworks and requirements within the European Union for a degree programme. Given the researched background, we propose a systematic way to implement knowledge, skill and competence objectives to a degree programme by using generally accepted frameworks. The framework targets engineering education in information technology, cyber security given on university level.

By having a well-established model for the degree programme, the private and public sector can flourish by having competent personnel at their use as employees.

CCS Concepts

• Social and professional topics→Model Curricula.

Keywords

Cyber Security; Education; Competence; Skill; Knowledge; European Qualifications Framework; Degree Programme.

1. INTRODUCTION

Workforce need for Cyber Security professionals has grown in the field of information technology with a fast pace. ICASA White Paper on the State of Cyber Security 2019 reports that the need for technical cyber security personel is rising and enterprises are struggling to fill their open positions [1]. According to the research from $(ISC)^2$ Cybersecurity Workforce Study report, the worker gap is 142 000 in Europe, the Middle East and Africa [2].

The education sector is under pressure to fulfil the needs to train competent workforce for the needs of industry. According to Burley et al. [3], cyber security degree programs are seen to be undeveloped. It seems that there is a lack of university level education in the field of cyber security. Cohen et al. pointed out in their paper that it is essential to recognize the demanded skills needed in government, industry and company levels [4]. Ciampa et al. argued in their paper that keeping the curricula up to date in relation to industry needs is very challenging [5] due to the fast development of ICT technology. Hence, threat vectors in cyber security also develop and change very rapidly.

CSIS - Center for Strategic & International Studies - publication from January 2019 shows critique to the education system about how Cyber Security is organized in the Education systems: "Organizations are also frustrated by the current cyber security education ecosystem, which lacks common metrics or rankings to help employers understand what programs, certifications, and degrees are the most effective." [6]. Raj et al. argue in their paper that it is crucial to standardize the cyber security curricula and the expected board of skills needs to be defined based on cyber security domain needs [7]. It can be undeniably said that there is a need for clear frameworks that describe the competence needs of the substance. After describing the skill needs, the model can be modeled under the curriculum to be built, which will ensure that the curriculum responds to the industry's competence needs and focuses sufficiently on the intended area of expertise.

In this paper, we researched the frameworks within Cyber Security education sector and the general frameworks regulating and guiding academic education in the area of the European Union. These frameworks are presented in chapter 2. The proposed model for designing a degree programme is established in chapter 3, and examples are given in chapter 4. Finally, we conclude with remarks on future research that should be conducted in this area.

2. EDUCATIONAL FRAMEWORKS

2.1 Frameworks in the European Union

Table 1. EQF terminology [8]

Skills	means the ability to apply knowledge and use know-how to complete tasks and solve problems. In the context of the EQF, skills are described as cognitive (involving the use of logical, intuitive and creative thinking) or practical (involving manual dexterity and the use of methods, materials, tools and instruments)
Knowledge	means the outcome of the assimilation of information through learning. Knowledge is the body of facts, principles, theories and practices that is related to a field of work or study. In the context of the EQF, knowledge is described as theoretical and/or factual
Competence	means the proven ability to use knowledge, skills and personal, social and/or methodological abilities, in work or study situations and in professional and personal development

ICETC 2019, October 28-31, 2019, Amsterdam, Netherlands.
©2019 Association for Computing Machinery.
ACM ISBN 978-1-4503-7254-1/19/10…$15.00
https://doi.org/10.1145/3369255.3369266

Within European Union the European Qualifications Framework (EQF) [8] EQF categorizes qualifications and competences into eight different levels, from EQF Level 1 to EQF Level 8. EQF also defines the characteristics of education to Knowledge, Skills and Competence, the explanations of which are given in table 1.

To harmonize, increase quality and enable student possibilities for multinational education within the EU, the member states are required to publish National Qualifications Frameworks [9]. These NQFs describe how current degree programmes within a member state map to the level requirements of the EQF.

ECTS User's Guide [10] describes and gives recommendations how degree programme supporting documents should be written. This is to promote transparency and transferability of studies within the European Higher Education Area (EHEA).

European Network for Accreditation of Engineering Education (ENAEE) gives out a framework for engineering education that ensures quality in all branches of engineering education [11]. EUR-ACE® label is awarded to degree programmes as a sign of quality of the degree programme. EUR-ACE categorizes the Programme Outcomes into eight learning areas, which are same for both the Master's Degree and the Bachelor's Degree:

- Knowledge and Understanding - KU
- Engineering Analysis - EA
- Engineering Design - ED
- Investigations - IN
- Engineering Practice - EP
- Making Judgements - MJ
- Communication and Team-working - CT
- Lifelong Learning – LL

Additionally, in the home country of the writers, the Finnish Cyber Security strategy insists that cyber security skills should be a part of all education levels of the Finnish education system [12].

2.2 Education Frameworks within the Cyber Security

Cybersecurity education Joint Task Force (JTF) has launched curriculum guidelines for post-secondary degree programs in cybersecurity [3] where the Association for Computing Machinery (ACM), IEEE Computer Society (IEEE-CS) and Association for Information Systems Special Interest Group on Information Security and Privacy (AIS SIGSEC) combined their views on curriculum development. The report also takes into account the different knowledge areas of cyber security. The report also presents well the wide range of knowledge's and the complexity of cyber security as it also has to take into account the relation to the IT environment where the needed cyber security skills are applied. Thus, in curriculum development one needs to accurately select the skills and abilities that one is aiming to educate. The overall picture of cyber security is too wide to be covered by one curriculum.

Internationally recognized accreditation body for engineering programs (ABET) has proposed the accreditation criteria for cybersecurity [13].

In Comprehensive National Cybersecurity Initiative [14] US President Barack Obama recognized cybersecurity as a critical challenge of economic and national security. By that recognition National Initiative for Cybersecurity Education (NICE) was initiated with the idea that an important resource in cyber resilience are the people with appropriate skills [15].

NICE framework is published by The National Institute of Science and Technology (NIST) [16]. Fundamentally NICE originates and focuses on the US; however the global nature of cyberspace is noticed there by partnering and global communities [15].

NICE framework describes and categorizes the work in cybersecurity into Work Roles and tasks assigned to those Work Roles. Those tasks require certain Knowledge, Skills and Abilities shortened as KSAs. With the mapping of KSAs to work roles, Educators can have awareness of how to map them into current course curricula. As stated in [15] "*Educators and trainers can use the framework to help answer these critical questions: What am I preparing my students for? What knowledge and skills do they need? What should I be teaching?".* In this study, that mapping is carried out as the design approach for a Degree Programme in Cyber Security.

The National Security Agency in the United States recognises two types of Centers of Academic Excellence (CAE): one in Cyber Defence (CAE-CD) and one in Cyber Operations (CAE-CO). NSA lists these degree programmes on their webpages, acknowledging the degree programme's quality, however, NSA does not directly fund the degree programmes. [17]

Cyber Defence (CAE-CD) consists of Knowledge Units. These Knowledge Units have been assigned to fit into NICE Framework Categories [18]. The Knowledge Units are for example:

- Cybersecurity Principles - SPY
- Basic Cryptography - BCY
- Security Program Management - SPM
- Basic Cyber Operations - BCO

Cyber Operations has only the criteria for measurement according to NSA [19] [20] but no valid Knowledge Units could be found during the writing of this paper. National Cyberwatch Center of the United States hands out a guide for mapping degree programme courses to the Knowledge Units of CAE-CD [21]. Based on the presentation "What They Are Teaching Kids These Days - Comparing Security Curricula and Accreditations to Industry Needs" at Black Hat 2017 [22], the degree field of the United States is in discussion how to implement Cyber Security in to their degree programs.

3. PROPOSED MODEL FOR DESIGNING A DEGREE PROGRAMME IN CYBER SECURITY

Given the developments of different frameworks into the field of Cyber Security, we propose the following model for Educational Organizations given in figure 1.

The Programme Outcomes of ENAEE are described as competences of the degree programme. In order to achieve these outcomes the courses are mapped to develop these competences accordingly to their degree level. Degree levels are mapped to the European Qualifications Framework according to National Qualifications Framework.

NICE Framework gives strict Work Role ID's that demand the development of certain Knowledge, Skills and Abilities to perform in given tasks assigned to the Work Role ID. These KSAs should be distributed as learning outcomes for the courses within the degree programme. These outcomes are also mapped to competences.

The development of the learning situations, laboratory exercises and types of assessment is left for the given course lecturer to choose the pedagogical solutions, which might include e.g. personal or group assignments, presentations, essays and exams.

Nonetheless the assignments should always develop the learning outcomes of the course. In addition, whatever evaluation method is used, it should assess the students' capability in the given NICE Knowledge, Skill or Ability.

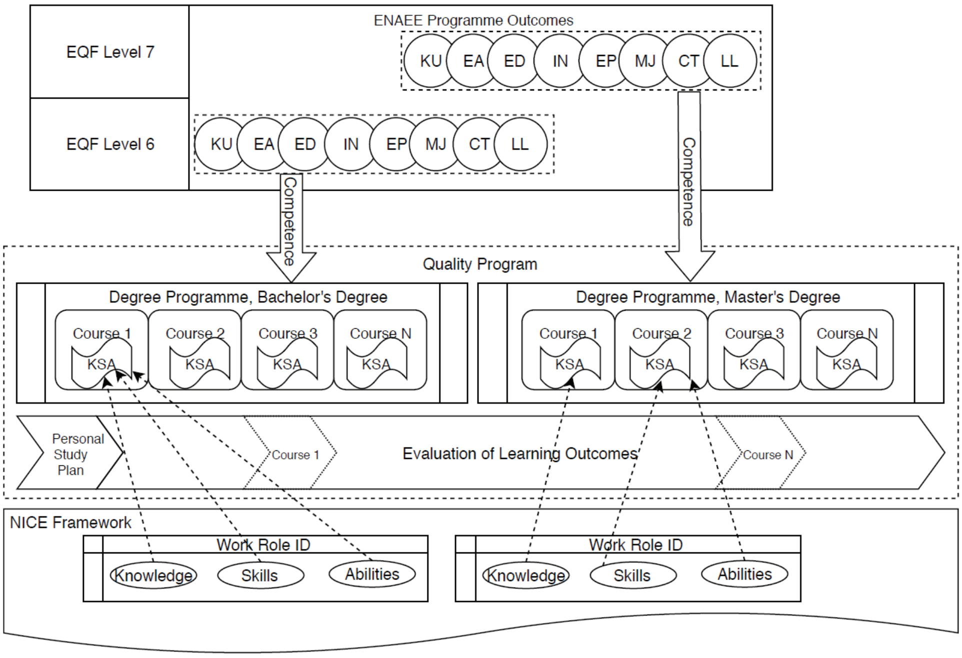


Figure 1. Model for Cyber Security Education Framework.

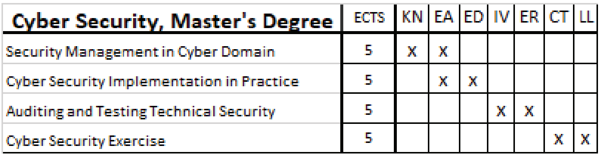
4. RESULTS

4.1 Competences

Competences should be mapped to different courses as described earlier in chapter 2. The ECTS User's Guide also promotes that these should be recorded as the learning outcomes of the programme. In our course descriptions these are seen as the competences -field.

In table 2, we present our mapping of the ENAEE competence model and how it is brought down to our Master's Degree courses in our degree programme at JAMK University of Applied Sciences [23].

Table 2. Competence Mapping to Courses



Cyber Security, Master's Degree	ECTS	KN	EA	ED	IV	ER	CT	LL
Security Management in Cyber Domain	5	X	X					
Cyber Security Implementation in Practice	5		X	X				
Auditing and Testing Technical Security	5				X	X		
Cyber Security Exercise	5						X	X

In our model the last course, Cyber Security Exercise, summarizes the degree programme and promotes life-long learning competence. The student, under the guidance of an educator, can evaluate all the earlier competences in the exercise, run in a safe learning environment.

Given table 2, the following chapters give examples as a case study for the Cyber Security Implementation in Practice course [24].

4.2 Learning Objectives

The learning objectives in our model are a double-edged sword. In the ENAEE competence model, we have generalized competences that every engineer should possess. In NICE framework, we have very specific tasks that competent personnel should handle in the field of Cyber Security. The Learning Objectives in the course description should have the best of both worlds.

Cyber Security Implementation in Practice course [24] has had cryptography as a field of implementation: How are mathematical algorithms are written in different computer languages and how cryptographic material is stored and used in computer systems? This learning objective is tied to two different work roles (as an example) in NICE:

- Cyber Defense Analyst (PR-CDA-001)
  - Knowledge of cryptography and cryptographic key management concepts, K0019
- Communications Security (COMSEC) Manager (OV-MGT-002)
  - Knowledge of encryption algorithms, K0018
  - Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g. S/MIME email, SSL traffic), S0138
  - Ability to manage Communications Security (COMSEC) material accounting, control and use procedure, A0165

In the ENAEE competence model, these tie to Engineering Analysis: how do the algorithms work and are written? The understanding of what different dependencies computer systems have in the written cryptographic libraries. They are also bound to Engineering Design competence on how to manage the cryptographic material in different computer systems and how it is created, distributed and used within the organization. This is summarized by the Learning Objective of Cryptography in Computer Systems.

Thus, the KSAs that NICE framework presents are mapped to learning objectives that are presented in the curriculum's course description in the learning outcomes -field.

4.3 Learning Situations & Assessment

Given student assignments should reflect the learning objectives. In the Cyber Security Implementation in Practice -course, the cryptography topic is further delved into with having lectures on the subject, classroom implementations as step-by-step guides followed by a research/implementation paper written on the chosen topic by the student. The written paper is then peer-reviewed and graded in the course by a fellow student. The lecturer grades the paper, multiple peer reviewers grade the paper, and the grade is then given for the whole assignment using a mathematical equation agreed at the start of the course.

Lectures increase knowledge, but also by writing and peer reviewing the student's understanding is further enhanced. Step-by-step classroom implementation enhances the theory into implementation skills, and the given implementation or research project enhances the ability to take this knowledge and skills into use. Understanding of the phenomenon further enhances as the students peer review each other's work.

As stated earlier, the learning situations can be from lectures to increase Knowledge and Understanding, to Investigations on researching and writing research/implementation papers, however, to enhance Communications and Team-working, full cyber security exercises could be run by the degree programme.

The assessment should concentrate on the KSAs assigned for the course and also be visible to the students in the course description. Different taxonomies such as Bloom's [25] or Solo's [26] Taxonomy could be used for assessing the levels of learning.

Technical competences were highly demanded in the background literature [1] [2] [4]. Based on our experience, a technical cyber range should be implemented to fully grasp the concepts of Cyber Security. Individual laboratory exercises can, in our opinion, develop the understanding and skills of some technical detail; however, cyber security often covers the interdependency of multiple technical details. Such interdependency, and resilience to withstand problems facing that interdependency, can only be taught in a realistic cyber environment, often called a cyber range.

At JAMK University of Applied Sciences in the Master's Degree programme [23], the competences are developed and can be publicly viewed. In addition, different courses can be further examined on what NICE KSAs they develop [27] [24] [28] [29].

Quality of the Degree programme should be monitored by the Quality Program within the Education Organization. In the European Union we recommend official accreditation programs such as ENAEE EUR-ACE® -label.

5. DISCUSSION

As the need for cyber security expertise grows in the industry, the need for an up-to-date degree program also increases. It is vital that when building the curriculum, the degree program should use some existing generally accepted framework researched from the industry. As the field of cyber security is broad, these frameworks help to focus on the learning objectives in the curriculum.

By providing good education on a well-established model, we can provide students a with a well-organized study path and the industry with clear visibility on the developed competences of the student. Increasing the performance of both the student and the industry.

Thus, we have mapped the EQF framework into our curricula and accredited one of the curricula by ENAEE, EUR-ACE –label. In this research paper, we mapped the curriculum courses to NICE framework to ensure that our degree programme is up-to-date and the education meet the needs of the industry. NICE framework is an extensive and multidimensional frame that can be used as a guideline for scoping the degree program and to ensure that the learning outcomes meet the industry demands.

Given the wide variety of different frameworks, some more specified to cyber security than others, the terminology within the frameworks overlaps, has different meanings and the interpretation is left to the reader. One example is Knowledge from the EQF which translates in ENAEE as Knowledge and Understanding. Another is Abilities in the NICE Framework, while EQF only recognizes Knowledge, Skills and Competence.

One inconsistency of the NICE Framework is that one singular knowledge is too specific and another one is too broad. As an example of this, the Knowledge of computer algorithms (K0015) is very abstract. However, encryption algorithms do not count as computer algorithms as they are categorized as a different Knowledge's (K0018)?

In our opinion, the knowledges expand from EQF level to another, further deepening the students' grasp of the concept. Thus, even though it isn't a part of the learning outcomes of a course, or an item of assessment, it should not be completely discarded from the course. This gives many interpretation problems for the teacher of the course and might be seen as an inconsistency of the degree programme.

In addition, some courses (e.g. the Cyber Security Exercise [27]) in the degree program, are so vast that they develop multitude of different knowledge, skills and abilities. These cannot be all evaluated within the course but are known to develop during the course. These cases are problematic to describe in the course description.

6. FUTURE WORK

Cyber Security is taught in the area of the EU; however future research should be made to study different competence models and course descriptions within those educational organizations. We know that in the area of ICT the labor force can move globally; hence, the research should also compare degree programs between the EU and for example USA or Asia.

One aspect for the future research is also to study how the students achieve the NICE KSA skills, brought down to the degree programme by this model, by conducting a survey study with the students attending the programme. In the survey, the student experience of the learning outcomes could be measured to reflect the NICE KSAs given for the course.

In addition, the workforce needs change based on the physical locations of the education organization, thus maybe the frameworks of describing cyber security workforce should differentiate between the locations. Further market inquiries could be made on how to match the industry needs of a location.

7. REFERENCES

[1] *State of Cybersecurity 2019: Current Trends in Workforce Development*. 2019. White Paper. ICASA.

[2] $(ISC)^2$ *Cybersecurity Workforce Study*. 2018. $(ISC)^2$.

[3] Burley, D., Bishop, M., Buck, S., Ekstrom, J., Gibson, D., Hawthorne, E., Kaza, S., Yair, L., Mattord, H. and Parrish A. *Curriculum Guidelines for Post-Secondary Degree*

Programs in Cybersecurity. 2015. DOI=http://doi.acm.org/10.1145/3184594

[4] Cohen, B., Albert, M.G. and McDaniel, E.A., 2018. *The Need for Higher Education in Cyber Supply Chain Security and Hardware Assurance*. International Journal of Systems and Software Security and Protection (IJSSSP), 9(2), pp.14-27.

[5] Ciampa, M. and Blankenship, R., 2019. *Do Students and Instructors See Cybersecurity the Same? A Comparison of Perceptions About Selected Cybersecurity Topics*. International Journal for Innovation Education and Research, 7(1), pp.121-135.

[6] *The Cybersecurity Workforce Gap*. 2019. CSIS.

[7] Raj, R.K. and Parrish, A., 2018. *Toward Standards in Undergraduate Cybersecurity Education in 2018*. Computer, 51(2), pp.72-75.

[8] COUNCIL RECOMMENDATION of 22 May 2017 on the *European Qualifications Framework for lifelong learning*. 2017. Retrieved March 20, 2019 from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&qid=1552997420044&from=EN

[9] *Government Decree on the National Framework for Qualifications and Other Competence Modules*. 2017. Finland. Retrieved April 2, 2019 from https://www.oph.fi/download/182107_Government_Decree_120-2017_27.2.2017_.pdf

[10] *ECTS Users' Guide*. Publicatins Office of the European Union. DOI=https://www.doi.org/10.2766/87192

[11] *EUR-ACE® Framework Standards and Guidelines*. 2015. ENAEE. Retrieved April 1, 2019 from https://www.enaee.eu/wp-assets-enaee/uploads/2017/11/EAFSG-Doc-Full-status-8-Sept-15-on-web-fm.pdf

[12] *Finland's Cyber security Strategy*. 2013. Ministry of Defence. Retrieved March 21, 2019 from https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

[13] Proposed Accreditation Criteria for Cybersecurity Academic Programs, ABET, Inc., Nov. 2017, [online] Available: www.abet.org/blog/news/abet-seeks-feedback-on-proposed-accreditation-criteria-for-cybersecurity-academic-programs

[14] United States. White House Office, *Comprehensive National Cybersecurity Initiative*, Apr 2010.

[15] C. Paulsen, E. McDuffie, W. Newhouse and P. Toth, "*NICE: Creating a Cybersecurity Workforce and Aware Public*," in *IEEE Security & Privacy*, vol. 10, no. 3, pp. 76-79, May-June 2012. DOI=https://www.doi.org/10.1109/MSP.2012.73

[16] *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.* 2017. NIST. DOI=https://doi.org/10.6028/NIST.SP.800-181

[17] Centers of Academic Excellence in Cybersecurity. Retrieved April 2, 2019 from https://www.caecommunity.org/content/what-is-a-cae

[18] Centers of Academic Excellence Cyber Defence Knowledge Units. Retrieved March 27, 2019 from https://www.iad.gov/NIETP/documents/Requirements/CAE-CD_2019_Knowledge_Units.pdf

[19] Criteria for Measurement for CAE in Cyber Operations Fundamental. NSA. Retrieved March 27,2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-fundamental/

[20] Criteria for Measurement for CAE in Cyber Operations Advanced. NSA. Retrieved March 27, 2019 from https://www.nsa.gov/resources/students-educators/centers-academic-excellence/cae-co-advanced/

[21] *A Guide for Mapping Courses to Knowledge Units. National Cyber Watch*. Retrieved March 27, 2019 from https://www.nationalcyberwatch.org/ncw-content/uploads/2017/12/NCC_Resource_Guide_A_Guide_for_Mapping_Courses_to_Knowledge_Units_v2.pdf

[22] Olson, R. and Sanders, C. *What They're Teaching Kids These Days*. 2017. Retrieved March 27, 2019 from https://www.blackhat.com/docs/us-17/wednesday/us-17-Sanders-What-Theyre-Teaching-Kids-These-Days-Comparing-Security-Curricula-And-Accreditations-To-Industry-Needs.pdf

[23] Master's Degree Programme in Information Technology, Cyber Security. 2019. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_rakenne_julkaisu.rakenne_komp_osaamisalue?ckohj=YTC&csuunt=99999&cvuosi=9S&caste=J&cark=2019-2020&lan=e

[24] Cyber Security Implementation in Practice. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0200&knro=&ark=&lan=e

[25] Bloom, B. S., Engelhart, M. D., Furst, E. J., Hill, W. H. and Krathwohl, D. R. (1956) *Taxonomy of educational objectives Handbook 1: cognitive domain*. London, Longman Group Ltd.

[26] Biggs, J. and Collis, K. 1982. *Evaluating the Quality of Learning The SOLO Taxonomy (Structure of Observed Learning Outcome)*. Academic Press.

[27] Security Management in Cyber Domain. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0100&knro=&lan=e&ark=

[28] Auditing and Testing Technical Security. Course Information. JAMK University of Applied Sciences. Retrieved April 18, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0300&knro=&lan=e&ark=

[29] Cyber Security Exercise. Course Information. JAMK University of Applied Sciences. Retrieved April 12, 2019 from https://asio.jamk.fi/pls/asio/asio_ectskuv1.kurssin_ks?ktun=YTCP0400&knro=&ark=&lan=e

VIII

CONVERSION OF EMERGING ICT TECHNOLOGY INTO CURRICULUM COURSES

by

Mika Rantonen & Mika Karjalainen, 2020

Journal of Strategic Innovation and Sustainability, 15(3), 70-77.

DOI: 10.33423/jsis.v15i3.2949

Reproduced with kind permission by JSIS.

CONVERSION OF EMERGING ICT-TECHNOLOGY INTO CURRICULUM COURSES

M. Rantonen,

JAMK University of Applied Sciences (FINLAND)

M. Karjalainen

JAMK University of Applied Sciences (FINLAND)

The aim of this paper is to describe the process of how to develop course content for a new challenging and emerging ICT technology in a higher education organization. The structure of the developed data analytics (DA) and Artificial Intelligence curriculum (AI) as well as the contents of the courses will be presented precisely. In spring 2017, the Institute of Information Technology at JAMK University of Applied Sciences started to develop its competence in DA and AI. The lack of good and well-organized university level education material and knowledge of the previously mentioned technology were the major challenges during the development process. Basic and very high-level theoretical courses from DA and AI can be found easily; however, hands-on type implementation courses were missing.

Keywords: Artificial intelligence, Data analytics, curriculum courses, Big Data, emerging technology, virtual courses

INTRODUCTION

AI has appeared in the field of ICT as an emerging technology in recent years, and the term seems to be on almost everyone’s lips. High expectations have been set for AI, which has reached a level of maturity where it can be applied to almost all industry areas.

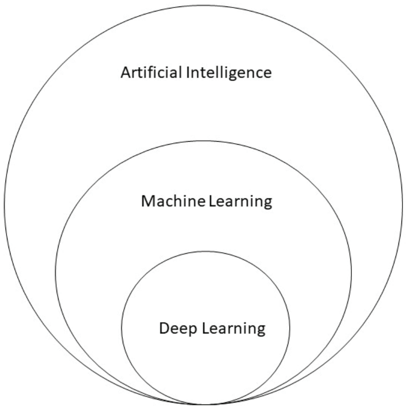
JAMK University of Applied Sciences (JAMK) started in the spring of 2017 with the help of internal funding to develop the expertise in data analytics (DA) and Artificial Intelligence (AI). The Institute of Information Technology at JAMK has invested in developing and applying its expertise in DA and AI for different areas and substances. The emphasis has been placed on the practical application of open source DA and AI products, either based on available open data or on real business-based problems. The challenge of bringing in the students to practice hands on work in the above-mentioned fields has been caused by the lack of educational courses at JAMK. The research team's approach to learning things has been hands on training, which has proven to be a very good solution. Knowledge has been gained precisely by doing, because every object of both application areas differs in some way from another object. The application of DA and AI differs significantly from the traditional use of program libraries in that the application of AI requires a profound knowledge of the applicability of various machine learning (ML) methods and neural networks to the problem to be solved. Knowledge of theory alone is not enough; developed AI methods must be tested in practice. In addition to the practical hands on work of the research team, it was noticed that the prolific knowledge can be transformed into courses that can be used in the future for university-level teaching.

METHODOLOGY

Modern information technology, incremental computing power, and online digitalization have opened new opportunities to utilize automatically collected and stored data from various sources. The exponentially growing amount of data is referred to as a Big Data and the traditional software and tools are not anymore applicable to process enormous amounts of unstructured data. Furthermore, the traditional computational pattern discovery of data mining is replaced with modern data analytics, ML and deep learning (DL) methods.

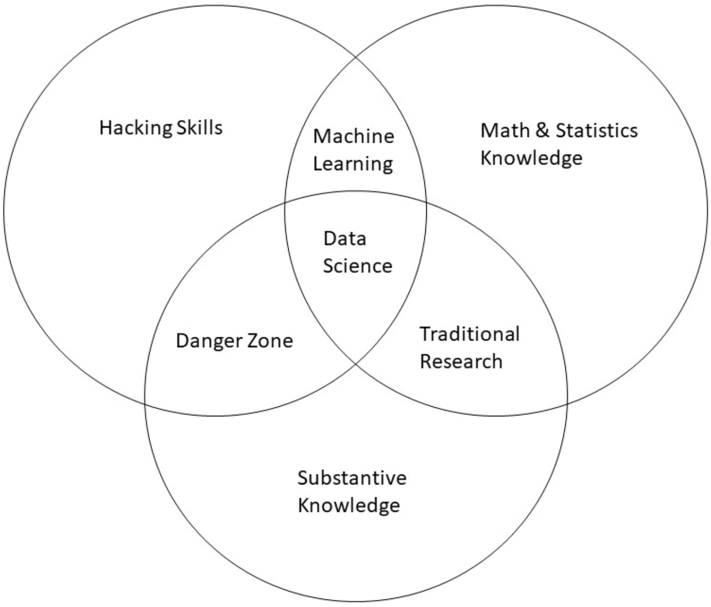
AI has existed over many decades, and the field is enormously wide (Goodfellow, 2016). AI can be viewed as an umbrella term that contains ML and DL. The ML is a subset of AI; meanwhile, DL, in turn, is a subset of ML (Fig. 1). The term DL refers to artificial neural networks (ANN) with complex multilayers (Abiodun, 2018).

FIGURE 1
A VENN DIAGRAM SHOWING THE RELATIONSHIP BETWEEN AI TERMINOLOGY.



Respectively, data science/analytics is a relatively new industry, albeit the fact that its components have been around for a long time. Venn diagram (Fig. 2) is used to understand that data science is a combination of several disciplines. In this Venn diagram, the three components are hacking skills, math & statistics knowledge, and substantive expertise (Conway, 2013), (Silver, 2018).

FIGURE 2
A VENN DIAGRAM SHOWING THE RELATIONSHIP BETWEEN DATA ANALYTICS/SCIENCE AND OTHER SKILLS.



Defining the data science/analysis skills is the split between substance and methodology which are ambiguous and unclear in how to distinguish among hackers, statisticians, subject matter experts, their overlaps and where data science fits. Therefore, a fully competent data scientist/analyst needs lots of different kind of a very extensive skill set. JAMK's approach to learning things has been hands on training, which has proven to be a very good solution. Knowledge has been gained precisely by developing different kind of applications and use cases. The application of DA and AI differs significantly from the traditional use of program libraries in that the application requires a profound knowledge about the data and domain. Knowledge of theory alone is not enough; developed DA and AI methods must be selected carefully and tested in practice. In addition to the practical hands on work of the research team, it was noticed that the prolific knowledge can be transformed into courses that can be used in the future for university-level teaching. Due to the requirements of skills, the courses and contents have been derived from the developed DA and AI applications and use cases.

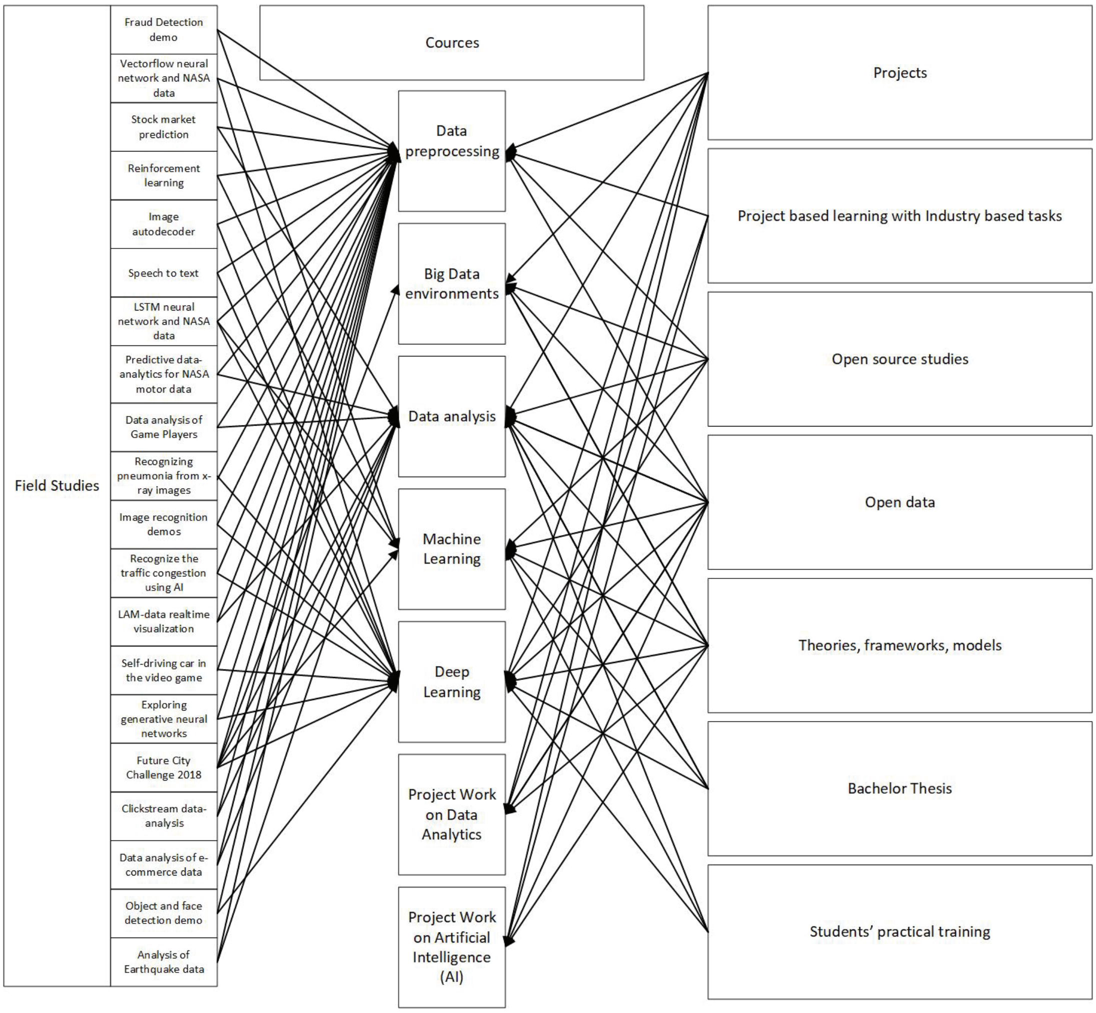
RESULTS

Development process and Framework of education courses in DA and AI

JAMK has responded to the lack of practically oriented educational courses in the area of DA and AI by introducing a 30-ECTS course offered by the Open University of Applied Sciences in autumn 2019. At the curriculum course developed there has been used the hermeneutic circular method (Dickens, 1977). In this case, by the literature review and general study from the area have been generated a general understanding of the area applicable. After review phase the understanding have deepened through a series of practical tests that have applied prior understanding of the area. In this way the curriculum frame has been built through the in-depth knowledge through exercises. Furthermore, Cross-industry standard process for data mining, known as CRISP-DM (Shearer, 2000) is an open standard process model that describes common approaches used in data mining, data analytics and deep learning projects. CRISP-CM has been used the map special skills and understanding using the developed framework to the specific curriculum course.

The content of the courses is designed based on the experience gained by a research team in the past 2 years regarding DA and AI. The course table consists of seven different completely virtual courses. All courses contain a lot of practical exercises, as is customary in Bachelor of Engineering type of education. Figure 3. illustrates the Framework of course development, describing the operating environment, the different sources and the working methods with which the courses have been developed. Based on the field's studies and different dataset, the Framework is applied and courses are defined to cover all needed skills.

FIGURE 3
FRAMEWORK OF COURSE DEVELOPMENT


Field Studies
Fraud Detection demo
Vectorflow neural network and NASA data
Stock market prediction
Reinforcement learning
Image autodecoder
Speech to text
LSTM neural network and NASA data
Predictive data-analytics for NASA motor data
Data analysis of Game Players
Recognizing pneumonia from x-ray images
Image recognition demos
Recognize the traffic congestion using AI
LAM-data realtime visualization
Self-driving car in the video game
Exploring generative neural networks
Future City Challenge 2018
Clickstream data-analysis
Data analysis of e-commerce data
Object and face detection demo
Analysis of Earthquake data
Cources
Data preprocessing
Big Data environments
Data analysis
Machine Learning
Deep Learning
Project Work on Data Analytics
Project Work on Artificial Intelligence (AI)
Projects
Project based learning with Industry based tasks
Open source studies
Open data
Theories, frameworks, models
Bachelor Thesis
Students' practical training

Field studies

JAMK's Data Analysis and Artificial Intelligence website (Artificial intelligence and data analysis, 2020) has published an example application with source code and data sets for those interested in it. The purpose of the sites is to provide information on applications, capabilities and examples of DA and AI that anyone can test according to their own interests. The idea behind the application examples was to use different kind of data and DA and AI methods as well as to find the core competencies of the development of DA and AI applications.

At the field study of fraud detection demo we took the credit card fraud detection as a case by using data classification based on neural networks. The focus of this field study was to recognize misuses of credit card using the information of transactions where the timestamp and amount of money are not anonymized (Credit card fraud demo, 2018). At vectorflow neural network and NASA data field study case, we tested vectorflow neural network-based prediction of engine failure in NASA motor data (Vectorflow RUL prediction demo, 2018). Furthermore, LSTM (Long short-term memory) neural network and Predictive data-analysis are used to predict the engine failure base on NASA motor data (Reamaining Useful Life (RUL) prediction, 2018) and (NASA motor data, 2018). In Predictive data analysis case, a linear regression and perceptons are used to predict the engine failure. At stock market prediction field study, we tested stock market prediction by using LSTM neural network to determine when to sell, buy or hold the specific stock based on the next day's closing price (Stock market prediction, 2018). At reinforcement learning we took the reinforcement learning method demo to teach worm movements in Worm game (Reinforcement learning, 2018). At image autodecoder use case, the neural network has been applied as an encoder to compress an image to floating point values. The decoder attempts to decompress their values back to an image resembling the original image (Autoencoder example, 2018). At Speech to text field experiment, speech to text translation where the learning scripts utilize the Tensorflow Dataset and Estimator APIs (Speech to Text with Neural Networks, 2018). Data analysis of Game Players study, data analysis of Battlegrounds players based on the movements and activities of players during the whole game duration were analyzed. Clustering method was used to categorize players' activity and success (Player Unknown´s Battlegrounds data analysis, 2018). At case recognizing pneumonia from x-ray images we used convolutional neural network (CNN) and transferred learning to recognize pneumonia with a small training data set (Predicting pneumonia from chest x-ray images with convolutional neural network, 2019). At case Image recognition demo, we use easy-to-use image recognition demos that work in a web browser. The open sets were used to teach the neural network developed using Keras (library). The loading of the model and the prediction were established by Tensorflow.js (Image recognition demos, 2020). At field study Recognize the traffic congestion using AI, AI based traffic congestion recognition was used. The road weather camera images of Finnish Transport Agency were fetched and the number of objects (cars etc.) was calculated using the neural network. The number of objects is visualized as a heat map on Google Maps (Traffic congestion demo, 2018). At field study LAM-data real time visualization, visualization demo application showed how to use deck.gl and react-map-gl to visualize LAM traffic data from Finnish Transport Agency's open data API (LAM-data visualization, 2019). At field study Self-driving car in the video game, the neural network is used to teach the self-driving car to drive independently on the video game tracks (Computer driven car in a simulated environment, 2018). At field study Exploring generative neural networks (GAN) we studied how neural networks can be used for creative purposes, such as synthesizing images from scratch. We explored generative models as a method of enhancing and drawing realistic human faces (Adversarial Generative models, 2018). At field study Future City Challenge 2018 JAMK, a student team made a proposal to the Future City Challenge (FCC) in Jyväskylä. The aim was to embrace resource wisdom city (Future City Challenge, 2018). At field study Clickstream data-analysis, clickstreams, also known as click paths, we study how the route visitors choose when clicking or navigating through a web site. Using data analytics, we examined the online shopping clickstream associated with the purchasing of products and sites from which Wikipedia has been accessed (Click path (Clickstream), 2018). At field study Object and face detection demo, object recognition used neural network either from the still images or video stream. Testing face recognition was integrated into the object recognition if the object is recognized as a person. Furthermore, the object recognition was integrated into the Nao robot (Face detection with TensorFlow object detection API, 2018). At field study Analysis of Earthquake data, data analysis and 3D visualization of earthquake data were performed (Clustering earthquake data, 2018).

Research and Development and Co-operation with Students

At JAMK, R&D in DA and AI in project form has started to grow as the expertise increases. Project preparation and application have been made possible by in-depth knowledge of DA and AI, both in theory and in practice, which enables us to make good applications to different funders. R&D at JAMK can be called applied R&D, which differs significantly from academic research in the university world. Applied R&D uses fully open source products and tools, which means applying existing ready methods to business problems. There is more academic and basic research in university research, going much deeper in algorithms or neural network architecture as in the applied R&D. The emphasis has been placed on the practical application of open source AI and DA products, either based on available open data or on a real business problem. The application of AI has been facilitated by the introduction of AI libraries by various commercial operators, perhaps best known as Google's Tensorflow (Tensorflow, 2020). In DA, the Python programming language is selected due to its well-known capability in conducting scientific calculation.

A research team consisting of staff and students is responsible for developing JAMK's expertise in DA and AI. Almost 20 Bachelor of Information and Communication Technology students have participated in the research group by completing a training or thesis in the field of DA and AI. Currently, 7 of them are working at JAMK as project staff, either in artificial intelligence or data analytics projects.

Projects and project based learning

In the spring of 2018, projects funded by the European Regional Development Fund (ERDF) were launched in the field of New Knowledge in Data Analysis and Business and Investments in a Data Security Development Environment. The projects aim to add value and new innovations to enterprise dark data through data analytics and machine learning methods. With the projects, the research team has built a secure data analytics and machine learning development environment. The project participants form a cluster of companies in the energy sector or closely related industries. The companies involved in the project are Fingrid, Alva (earlier Jyväskylän Energia), Landis+Gyr and C2Smartlight. The location of companies in the same field of industry enables data analytics and its utilization and development throughout the value chain: Production <-> Distribution <-> Consumption <-> Customers. The projects also include cases of common interest between companies seeking to combine corporate data and find synergies. In addition, JAMK has also carried out a research project directly funded by the National Defense Science Advisory Board (MATINE): Using Artificial Intelligence to Detect Anomalies in Web Traffic. In addition to these projects, JAMK uses a lot of project-based learning in teaching, where we have collaborated with several companies and gained experience of the need for different environments for artificial intelligence and data analytics.

Open source tools and data

JAMK has deliberately focused on using open source solutions, the release of which has accelerated the development of artificial intelligence in recent years. In addition, these have allowed for the full allocation of funding to skills development, without burdening licensing and software fees. Essential to vendor independence is also the avoidance of the so-called vendor lock, *i.e.* commitment to one and only cloud service or software provider.

The development of AI requires data to train ML models or neural networks. The amount of data can be substantial depending on the application. The most used environments are cloud-based, where scalable computing time, storage, and memory can be purchased. While the consumption of cloud computing, storage and memory is compared and pricing may be quite clear, it is very difficult to predict the overall cost in DA or AI projects. For example, when training a neural network, the cost of computing capacity may come as a surprise. Another issue that has emerged in business collaboration is data security, security and legal issues for cloud-based DA and AI environments. This has been the most common issue when it comes to the disclosure of corporate data. Companies want a guarantee that data is stored properly, and they may not want to put it in the cloud. An alternative is to build your own DA and AI environment. Costs of your own computing environment may be high; however, after that the costs consist mainly of maintenance and power consumption.

The clear challenge for practical implementation has been data, or indeed the lack of it. Both DA and AI need to have enough data and preferably still, enough quality data. Without data you cannot optimize DA algorithms or teach ML algorithms. For many companies, data sharing poses a challenge for three main reasons:

1. Data informs about their critical business and the company does not dare to divulge their data despite confidentiality agreements.
2. Data can be stored in many locations, meaning it is in multiple locations and very old systems, which it may be very cumbersome to collect it.
3. Data quality may be poor; i.e. there may be many missing values, duplicate values or values that do not exceed the rating scale. With such poor-quality data, it is almost impossible to make a good ML model

DA and AI Curriculum Courses

During the curriculum development process, the staff and students co-operate as a team and develop the ability to carry out concrete real-world DA and AI use cases. The diversity of the use cases provides a strong insight how the curriculum must be structured, and what kind of knowledge has to be included (Fig. 3).

The ability and knowledge in DA and AI are well documented and refined to 30-ECTS education and a part of the curriculum in ICT engineering education. The curriculum consists of the following courses:

- Data preprocessing, 3 credits
- Big Data environments, 5 credits
- Data analysis, 4 credits
- Machine Learning, 5 credits
- Deep Learning, 5 credits
- Project Work on Data Analytics, 4 credits
- Project Work on Artificial Intelligence (AI), 4 credits

The courses and the contents are derived from the field studies. Each field study is from a different domain and each of them has their own challenges. The challenges are mapped using Framework of course development to the specific course.

CONCLUSIONS

Precise knowledge of course contents has been gained hand on by doing, because every application of DA and AI differs in some way. Furthermore, the process of DA and AI projects varies significantly from a traditional ICT project as well as the use of DA or AI software varies from the use of traditional use of program libraries. The application of DA and AI requires a profound knowledge of the applicability of various ML methods and neural networks to the problem that is to be solved. Knowledge of theory alone is not enough; DA and AI must be tested in practice.

This continuous and iterative process of curriculum development has now been refined and is offered as 30-ECTS education in DA and AI which started in the fall of 2019 at the Open University of Applied Sciences. In the first implementation, only 35 participants were accepted, and the course was full within three minutes. The second enrolment started on 18 November 2019 with 100 study places and the course was full within eight hours. The first 45 study places were reserved in about 2 minutes. In addition, JAMK will launch a master's degree program in AI and DA with tuition in English in the autumn of 2020.

In the field of technology, the rapid development of technologies presents challenges for keeping teaching up to date. Basic research in the field of artificial intelligence has a long tradition, and we are now at the stage where technology maturity allows for a large-scale application. Thus, artificial intelligence and data analytics must be integrated into a modern engineering education. Educationally, taking over the aforementioned technology is a major challenge. By following the model presented in this paper, the know-how generated by practice can be generated into course structures. The use of the model is of prime importance, especially in the field of applied engineering, where the course content must provide an opportunity for the student to learn with hands on exercises and training.

REFERENCES

Abiodun, O. I. (2018). State-of-the-art in artificial neural network applications: A survey. *Heliyon*, 4(11).

Adversarial Generative models. (2018, 6). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/generative-adversarial-model-experiments

Artificial intelligence and data analysis. (2020, 3). Retrieved from https://jamk.fi/en/ai

Autoencoder example. (2018, 2). Retrieved from ttps://gitlab.labranet.jamk.fi/data-analysis-and-ai/autoencoder-demo

Click path (Clickstream). (2018, 6). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/da-documentation/tree/master/clickstream

Clustering earthquake data. (2018, 5). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/earthquake

Computer driven car in a simulated environment. (2018, 6). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/tmnf-car

Conway, D. (2013, 3). *The Data Science Venn Diagram*. Retrieved from http://drewconway.com/zia/2013/3/26/the-data-science-venn-diagram

Credit card fraud demo. (2018, 2). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/credit-card-fraud-demo

Dickens, D. (1977). *Hermeneutics and Ethnomethodology.*

Face detection with TensorFlow object detection API. (2018, 5). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/object-detection-demo

Future City Challenge. (2018, 4). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/FCC

Goodfellow, I. B. (2016). *Deep Learning.* MIT Press.

Image recognition demos. (2020, 3). Retrieved from https://aida2.labranet.jamk.fi/

LAM-data visualization. (2019, 10). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/lam-station-visualization

NASA motor data. (2018, 3). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/nasan_moottoridata

Player Unknown´s Battlegrounds data analysis. (2018, 5). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/PUBG-data-analysis

Predicting pneumonia from chest x-ray images with convolutional neural network. (2019, 5). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/pneumonia-cnn

Reamaining Useful Life (RUL) prediction. (2018, 2). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/nasa-rul-prediction-lstm

Reinforcement learning. (2018, 2). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/reinforcement-learning-demo

Shearer, C. (2000). The CRISP-DM model: the new blueprint for data mining. *Journal of Data Warehousing*, 13-22.

Silver, A. (2018, 9). *The Essential Data Science Venn Diagram*. Retrieved from https://towardsdatascience.com/the-essential-data-science-venn-diagram-35800c3bef40

Speech to Text with Neural Networks. (2018, 10). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/speech-to-text

Stock market prediction. (2018, 2). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/stock-market-prediction

Tensorflow. (2020, 3 17). *An end-to-end open source machine learning platform*. Retrieved from https://www.tensorflow.org/

Traffic congestion demo. (2018, 6). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/traffic-congestion

Vectorflow RUL prediction demo. (2018, 2). Retrieved from https://gitlab.labranet.jamk.fi/data-analysis-and-ai/nasa-rul-prediction-vectorflow

IX

AUTHENTIC LEARNING ENVIRONMENT FOR IN-SERVICE TRAININGS OF CYBER SECURITY: A QUALITATIVE STUDY

by

Mika Karjalainen & Anna-Liisa Ojala, 2021

International Journal of Continuing Engineering Education and Life-Long Learning.
Accepted/In print.

Reproduced with kind permission by IJCEELL.

Request a copy from author.