Advances in Science, Technology and Engineering Systems Journal
Vol. 5, No. 5, 592-600 (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: 10 August, 2020
Accepted: 15 September, 2020
Online: 05 October, 2020

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/aj050572

to be closed and totally controlled to allow risk free usage of real attacks and intrusions [13]–[14]. 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 [15]. As stated in [16], 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 [16] 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 [17]. 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 [18]. JYVSECTEC has also been Finland's representative in the Cyber Defence Pooling & Sharing Project of European Defence Agency (EDA) [19]–[20].

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 [21]. 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 [22]. 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 [23]. 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 [24]. 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 [25]. 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 [26]. 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 [27].

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 [28]. 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.

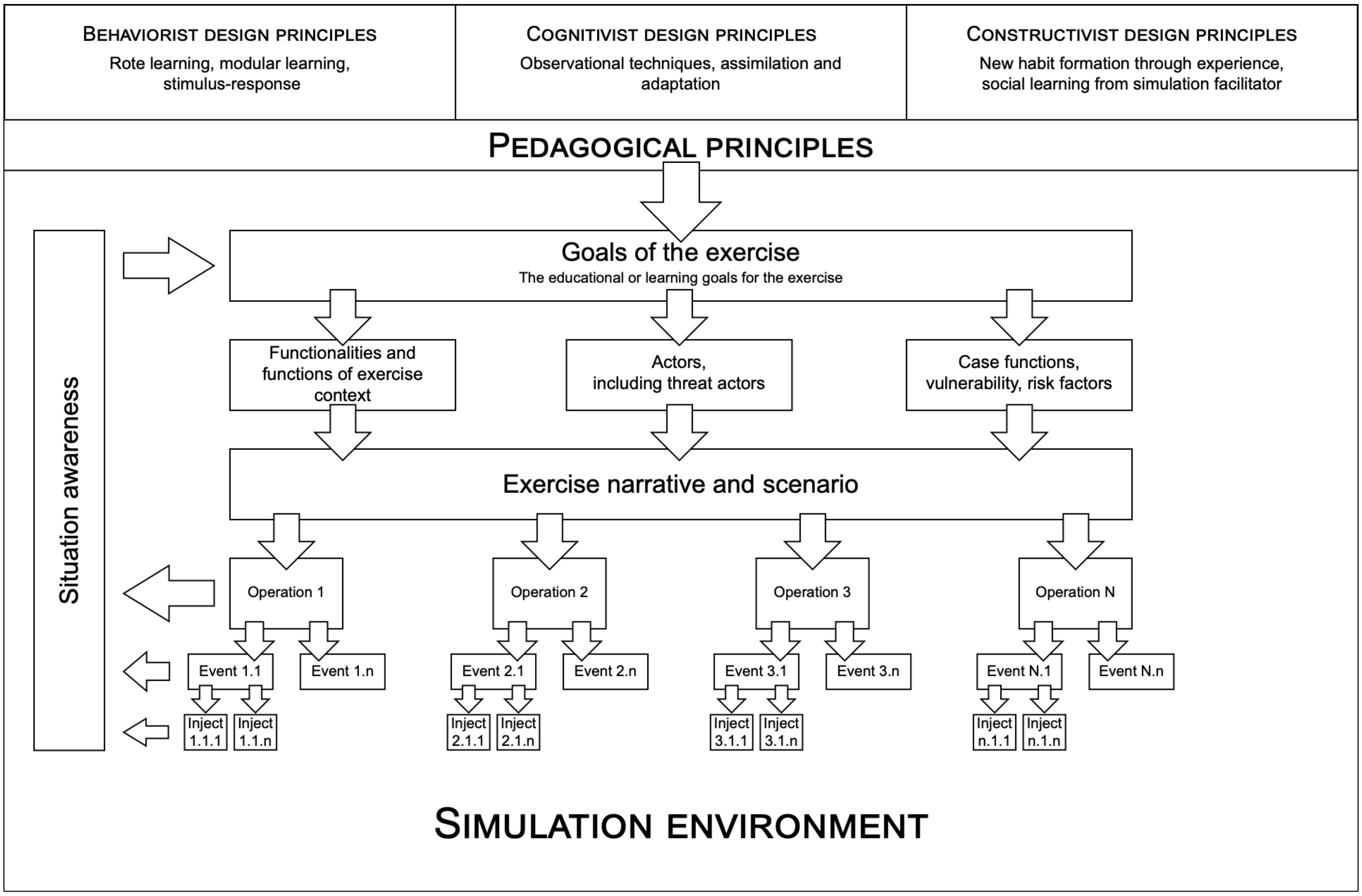

BEHAVIORIST DESIGN PRINCIPLES
Rote learning, modular learning, stimulus-response
COGNITIVIST DESIGN PRINCIPLES
Observational techniques, assimilation and adaptation
CONSTRUCTIVIST DESIGN PRINCIPLES
New habit formation through experience, social learning from simulation facilitator
PEDAGOGICAL PRINCIPLES
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 [29]. 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 [30]. 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 [31].

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 [32], 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) [33]. Consistently, MITRE describes three stages (Exercise Planning, Exercise Execution and Post Exercise) [34]. Vykopal et al. defines five stages for exercise; preparation, dry run, execution, evaluation, and repetition [35]. 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-

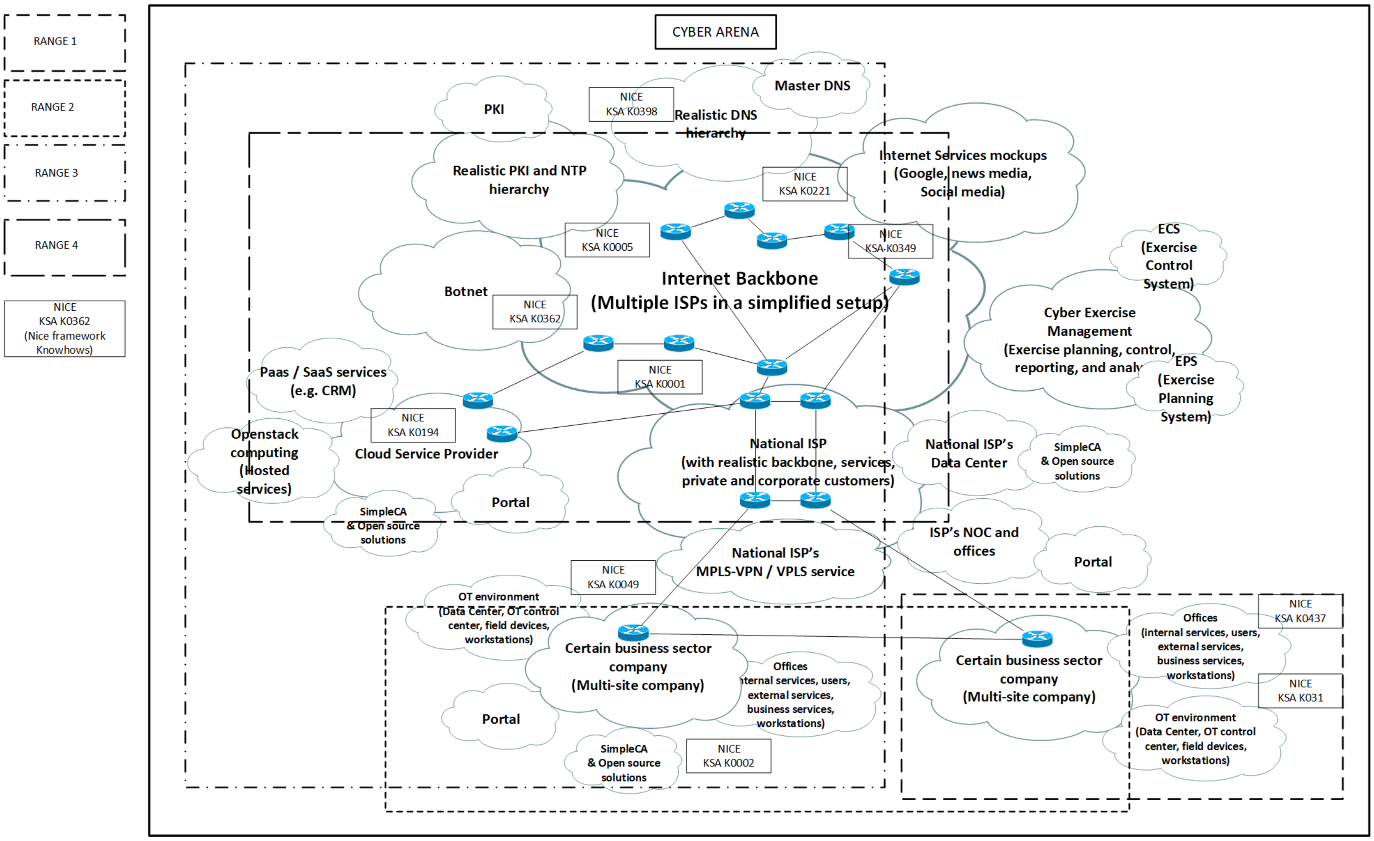

RANGE 1
RANGE 2
RANGE 3
RANGE 4
NICE KSA K0362 (Nice framework Knowhows)
CYBER ARENA
PKI
NICE KSA K0398
Realistic DNS hierarchy
Master DNS
Realistic PKI and NTP hierarchy
Internet Services mockups (Google, news media, Social media)
NICE KSA K0221
NICE KSA K0005
NICE KSA-K0349
Botnet
NICE KSA K0362
Internet Backbone (Multiple ISPs in a simplified setup)
ECS (Exercise Control System)
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
SimpleCA & Open source solutions
Portal
ISP's NOC and offices
Portal
National ISP's MPLS-VPN / VPLS service
NICE KSA K0049
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 [16]

ercise evaluation, and improvement planning [36]. 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

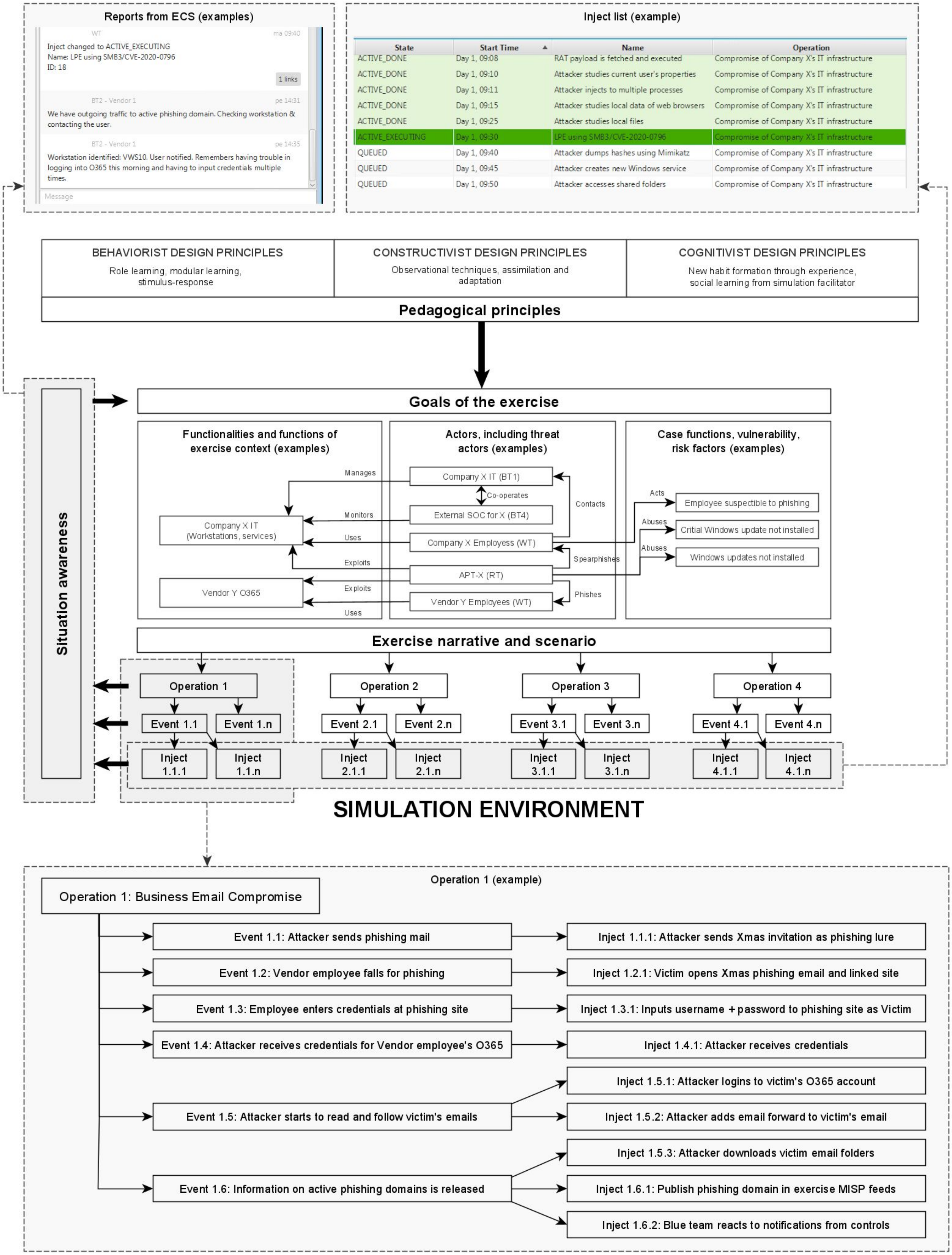
The first step of exercise life-cycle is the planning-phase. It is an extremely critical phase, because it determines the effectiveness of the whole exercise. From the viewpoint of competence development, the content of the exercise e.g. scenario, actors, and events shall be fitted to the requirements 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 [37] *"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 [38]. 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
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
Event 1.2: Vendor employee falls for phishing
Event 1.3: Employee enters credentials at phishing site
Event 1.4: Attacker receives credentials for Vendor employee's O365
Event 1.5: Attacker starts to read and follow victim's emails
Event 1.6: Information on active phishing domains is released
Inject 1.1.1: Attacker sends Xmas invitation as phishing lure
Inject 1.2.1: Victim opens Xmas phishing email and linked site
Inject 1.3.1: Inputs username + password to phishing site as Victim
Inject 1.4.1: Attacker receives credentials
Inject 1.5.1: Attacker logins to victim's O365 account
Inject 1.5.2: Attacker adds email forward to victim's email
Inject 1.5.3: Attacker downloads victim email folders
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) [39] and OODA-loop (Observation-Orientation-Decision-Action) [40, 41].

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 [42]. 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 [43] presents a framework for competence development and assessment in hybrid cyber security exercises, and the authors of [44] introduce one adoption of the Kirkpatrick Model.

Other methods for evaluating exercise can also be used, the authors of [45] 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 [46], 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 [47]. 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 [48] and Leahy et. al [49] 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 [50], 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] 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.

[15] 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.

[16] 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.

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

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

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

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

[25] 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.

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

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

[28] 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.

[29] 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.

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

[31] 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.

[32] 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.

[33] 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.

[34] 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.

[35] 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.

[36] 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.

[37] 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.

[38] 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.

[39] 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.

[40] 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.

[41] 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.

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

[43] 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.

[44] 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.

[45] 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.

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

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

[48] 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.

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

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