Authentic learning environments for in-service training in cybersecurity: a qualitative study

Mika Karjalainen* and Anna-Liisa Ojala

JAMK University of Applied Sciences,
P.O. Box 207, FI-40101, Finland
Email: Mika.karjalainen@jamk.fi
Email: Anna-liisa.ojala@jamk.fi
*Corresponding author

Abstract: Today's rapidly digitalising world has led to business processes becoming digitalised, which necessitates paying attention to the cybersecurity issues inherent in those digital processes. The multi-disciplinary nature of working life and the complexity of cybersecurity issues place demands on learning environments. The present study examined the requirements for optimal in-service training to ensure individual and organisational learning of the competencies that are crucial for dealing with cybersecurity incidents. Building on theories of authentic learning and qualitative research methods, the study identified three fundamental components and four elements of optimal in-service cybersecurity training. The research found that practicing organisational actions increased readiness and competence to act in the face of a real cybersecurity incident. A comprehensive cyber arena supports the implementation of optimal training and thus the efficiency of in-service training.

Keywords: cybersecurity; cyber arena; cyber range; authentic learning environment; training; exercises; peadagogy; in-service training.

Reference to this paper should be made as follows: Karjalainen, M. and Ojala, A-L. (2023) 'Authentic learning environments for in-service training in cybersecurity: a qualitative study', *Int. J. Continuing Engineering Education and Life-Long Learning*, Vol. 33, No. 1, pp.128–147.

Biographical notes: Mika Karjalainen is working in the Jyväskylä University of Applied Sciences as the Director of the IT-institute. He also leads the institute's cyber security research, development and training centre JYVSECTEC, which maintains and develops the Finnish national cyber security range, and has organised the Finnish National Cyber Security Exercise annually since 2013. He holds a PhD in Information Technology and conducting research in the field of cyber security education, specially focusing to students learning during the cyber security exercises.

Anna-Liisa Ojala holds a PhD in Social Sciences. She works currently as a project and research specialist in the School of Professional Teacher Education of JAMK University of Applied Sciences Jyväskylä, where she designs development projects and conducts studies on learning, professions, and youth cultures.

1 Introduction

The concept of cybersecurity became more widespread in the early 2010s, as the digitalising world introduced new threats. In addition to traditional cyber threats and digital influences on information, digitisation is now affecting almost all business processes in the Western world, and cybersecurity issues have increasingly become business process issues. This situation has created a need for cybersecurity specialists to ensure the security of business processes, which according to Lindsay et al. (2003) are multi-faceted, complex, and include human operators. These specialists must continually update their competencies as the technologies, threats, and operating environments in which they work evolve. Many cybersecurity experts work in occupations and positions, (e.g., as cybersecurity experts in banks) that seldom require them to face real-life cyber distractions and interference – situations that are referred to hereafter as *incidents*. Nevertheless, they should have the competence to recognise incidents and respond appropriately to them. To become experts, specialists require continuous in-service training to maintain and advance their expertise in today's rapidly changing world.

In the present study, we examined *the requirements for optimal in-service training implementation to ensure the individual and organisational competency learning that is crucial for facing complex real-life situations and maintaining business process performance in the case of cybersecurity incidents*. We focused on both the physical environment (including technology implementation) and pedagogical acts and interactions, which together enhance the pedagogical solutions of in-service training. In this paper, by business processes, we mean all commercial and non-commercial 'sets of partially ordered activities intended to reach a goal' (Hammer and Champy, 1993) performed by companies, public actors, and non-profit organisations. The present study was built on the concepts of learning proposed by Herrington and Oliver (2000) and Herrington et al. (2010), which underpin experiential learning theories (Engestrom, 2001; Kolb et al., 2001; Schon, 1987).

Section 1 discusses changes in operating environments and their effects on cybersecurity competence requirements and teaching. It also reviews the training and teaching platforms commonly used in cybersecurity education. Section 2 explains the pedagogical theories relating to cybersecurity training and its application. Section 3 describes the research process and the data it produced. Section 4 explains the results of the study, and Section 5 presents the conclusions that were drawn from them.

1.1 The context of the study

We first aimed to define the term cybersecurity and distinguish it from other previously used information security terms. The concept of cybersecurity initially referred to threats created by digital operating environments (Secretariat of the Security Committee, 2013). The difference between information security and cybersecurity can be expressed simply: information security focuses on ensuring the accuracy, integrity, and usability of the data, but the concept of cybersecurity extends the context and impact to digital operating environments and, through them, to the physical world (Von Solms and Van Niekerk, 2013). Over the past ten years, the concept of cybersecurity has been widely adopted and materialised (Enescu, 2019; Hatfield, 2018; Sisaneci et al., 2013) and has now become tied to global phenomena, individuals' experiences and environments, the operations of

companies and other organisations, and new technologies such as artificial intelligence or data analytics.

In the context of cyber environments, the blurring of the borders of traditional states is often highlighted (Guild et al., 2008) with regard to trends such as cloud technology, mobile devices, hacking, political attacks and opinion influencing in digital environments, cyber wars, and manipulation of information (Lupovici, 2011). Continuous, ever-accelerating change means that activities in cyber operating environments are likely to become more strictly regulated in the near future (Gantzias, 2020). A good example of this is the general data protection regulation introduced in the European Union (EU) in spring 2018.

In practice, expanding and increasingly complex digital operating environments have led to an exponential increase in vulnerabilities and the consequent need for increased resilience. In recent years, companies have begun to actively detect the new threat vectors introduced by digital operating environments and capitalise on the new business opportunities offered by such environments (Berman, 2012; Kurniawati et al., 2020).

1.2 Cybersecurity exercise platforms

A cybersecurity exercise platform (cyber range) is an information technology (IT) platform that allows research and development activities to be conducted and provides an environment that can be used for educational purposes. The exercise environment is a closed environment in which IT activities are simulated. In general, such an environment should be able to simulate internet structures, including user-generated traffic and realistic business environments, so that the IT and operational (OT) systems appropriate to operating environments can be modelled with their core functionalities. If more than one business environment needs to be modelled, the interdependence of the environments and the use of internet and/or cloud services can be simulated. Legislation imposes special requirements for the security of such environments; for example, the handling of real malware is only allowed by criminal law for authorities and research facilities, since these have recognised cyber exercise environments.

The need for such closed operating environments has been identified worldwide (Ministry of Defence Finland, 2019; The NATO Cooperative Cyber Defence Centre of Excellence Exercises, 2019; Uckan Farnman et al., 2015), and several cyber exercise ranges exist around the globe, with functionalities driven by technology, operations, and/or industry needs (Yamin et al., 2020). Thus, exercise platforms differ considerably from each other, making comparison between them difficult in terms of the added value of activities.

1.3 Previous studies

Several frameworks have been constructed to develop cybersecurity competencies and education, with NICE (the US National Initiative for Cybersecurity Education) being one of the most popular. Parrish et al. (2018) identified four domains of cybersecurity: *governance* (policy, strategy, compliance, and standardisation); *risk management* (threat modelling, asset evaluation, mitigation, and vulnerabilities); *constraints* (legal, ethical, organisational, political, and privacy-related) and *controls* (administrative, physical, and technical). Their study suggested a meta-disciplinary framework for cybersecurity to guide the implementation of cybersecurity programmes. Meta-disciplinary cybersecurity

refers to the various speciality areas, organisational structures, tasks that the cyber domain comprises. Dawson and Thomson (2018) discussed the physical, logical, and social layers in such a domain, which affect the success of cyber professionals. They also emphasised the need for training in social skills. In line with Dawson and Thomson's study, Lehto et al. (2017) and Kucek and Leitner (2020) also recommended recognising the human factors in cybersecurity. Additionally, the pedagogical mechanisms of curriculum development have been studied in relation to working life needs (Endicott-Popovsky and Popovsky, 2014). Despite these studies, which have emphasised the multi-disciplinary nature of cybersecurity domains, the human factors and social layers have rarely been studied or carefully examined by scholars. As explained in more detail in the methods section, the present study specifically investigated these factors and layers.

Over the past ten years, cybersecurity exercises have become a widely used pedagogical method of cybersecurity teaching. Although simulation pedagogy is an increasingly studied pedagogical field (Lathleiff, 2019; Rashid et al., 2019; Rystedt et al., 2019), research on cybersecurity exercises has mainly focused on the study of the technical manifestations or implementation methods of the exercises or the cyber ranges used for the exercises (Larrucea and Santamaría, 2020; Tian et al., 2018; Winter, 2012). Other closely related studies have reported on or examined the designs of degree programs for cybersecurity (Mouheb et al., 2019; Saharinen et al., 2019; Švábenský et al., 2018).

Research on cybersecurity exercises as tools for competency development has, until recently, been almost non-existent (Brilingaitė et al., 2020; European Commission, 2013; Karjalainen et al., 2019; Karjalainen and Kokkonen 2020; Maennel, 2020; Secretariat of the Security Committee, 2013). Karjalainen and Kokkonen (2020) considered the planning, implementation, and feedback phases of cybersecurity exercises from a pedagogical point of view. Like Karjalainen and colleagues (2019), they emphasised the need for complexity in the exercises to reflect the complexity of operating environments. Brilingaitė et al. (2020) summed up several aspects and dimensions of the exercise lifecycle and developed a framework for organising exercises, which, in our experience, is often used in practice. However, little is known about the factors that are critical for ensuring learning during such exercises. Pedagogical theories in particular are neglected in studies examining cybersecurity exercises. The present study filled this knowledge gap by examining these factors utilising authentic learning theory (Herrington and Oliver, 2000; Herrington et al., 2010).

2 Pedagogical framework: real-life experiences, reflection, and authentic learning environments

Ericsson (2008) in his theory of intentional practices [deliberated practice (DP)]; asserted that 'hands-on' training is a necessary part of the development of expertise. Experiential learning theory claims that experience is vital, but does not necessarily guarantee an effective learning experience. In addition to experience, a combination of thinking and new perceptions is needed (Kolb et al., 2001). Through new experiences and cognitive processing, learners are able to conceptualise and analyse competencies. Often, this is helped by the verbalisation of the learning event and the new thinking that emerges from

it through, for example, thinking aloud (Engestrom, 2001; Malinen, 2000; Schon, 1987). Experience of real-life situations and cognitive reflection are also crucial in professional cybersecurity.

Simulation pedagogy is one way to offer experiences to learners. It has a long tradition, especially in nursing and medical education, and increasingly in engineering education (Bariran et al., 2013; Emin-Martinez and Ney, 2013; Nystrom et al., 2016). The reason for these fields preferring simulation pedagogy is that it provides an opportunity to practice risky situations in a low-risk environment and improves expert performance and professional confidence in situations that professionals rarely face (Kalaniti and Campbell, 2015; Kong et al., 2017). However, as Kalanti and Campbell (2015) stated in their medical study, organising a simulated session is both time-and labour-intensive; hence, the optimal setup of the learning environment should be thoroughly considered.

Herrington and Oliver (2000) specified design requirements for a learning environment that simulates a real operating environment. According to them, teaching should offer authentic learning environments that reflect the same functionalities and requirements that the learner must consider when applying what he or she has learned in real life. The following are their requirements for a real learning environment:

1 An authentic context that describes or corresponds to the way in which knowledge and skills are used in real life.

2 Authentic activities that reflect the main content of the whole course or study unit.

3. Learners are provided with models of how to actually act in real-life situations.

4 Learners are enabled and encouraged to take on different roles and consider their learning and the environment from different perspectives.

5 Opportunities are provided for collaborative knowledge creation.

6 Opportunities are provided for learners to reflect on their levels of competence and learning relative to the context of the learning environment, authentic tasks, and expertise.

7 Opportunities are provided for students to articulate and justify their actions and choices to others.

8 Students are provided with community support for the learning process that does not oversimplify the learning environment but prepares and creates support structures for them to do things in a meaningful way.

9 Assessment of learning that is tightly integrated into activities, allowing learners to focus on activities and learning and to produce products and outputs in collaboration with others.

In the present study, we utilised these nine requirements for learning environments during the data collection and coding, as explained later in the text, and the study findings reflected these elements. Utilising these requirements enabled us to consider the field-specific requirements for learning environments in cybersecurity in-service training, including adequate simulation of the operating environment and the development of essential skills for learners.

3 Methods and data

Previous research determined the requirements for an optimal cybersecurity learning platform (Karjalainen and Kokkonen, 2020) and examined individuals' learning during a cybersecurity exercise, focusing on learners' competence before and after the exercise using a NIST NICE framework-based questionnaire (Karjalainen et al., 2019; Petersen et al., 2020). To deepen the understanding gained from previous studies, we studied the requirements for a cybersecurity learning environment by interviewing experienced cyber technology experts and utilising Herrington and Oliver's (2000) (see also Herrington et al., 2010) attributes of authentic learning environments to reflect on theory. Gaining access to a particular research site is not easy (Amis, 2005), especially when addressing topics that are subject to business confidentiality, but due to the first author's role in the Jyvaskyla Security Technology (JYVSECTEC) organisation, we were able to approach experts who might agree to be interviewed. Interviewing is a traditional method for examining how something has happened and why (Amis, 2005). In the present study, we used interviews to examine why cybersecurity experts with wide experience of designing and conducting cybersecurity in-service training designed and conducted them in the way they did and whether they identified areas for improvement. The face-to-face interviews were conducted online in spring 2020, using Microsoft Teams, due to the COVID-19 pandemic.

The data was drawn from five semi-structured interviews with experts from JYVSECTEC. The interviews consisted of two phases. The first phase started with questions about the interviewee's experience as a specialist and range developer, then proceeded to explore their perceptions of how the range served (or did not serve) customers' needs. In the second phase, the attributes of an authentic learning environment (Herrington and Oliver, 2000) were presented one-by-one to the interviewees on PowerPoint slides, with each slide introducing one attribute, translated into Finnish. Two questions were asked for each attribute:

1 How do the range and the cybersecurity practices put this attribute into practice?

2 Could something be done better in the future?

The interviews lasted from one hour and two minutes to two hours and 18 minutes. They were recorded, transcribed, and conducted in Finnish. The interviews were conducted by the second author, who had no previous connection to the informants. The first author and the informants were colleagues, which we considered might cause a risk of bias during the data collection. The informants were aware of the researchers' identities, and all of them were independently informed that there were no conflicts of interest, although the first author would be able to identify the informants. However, the first author only had access to the transcribed data, which was anonymised.

The analysis began by coding the data. Coding can be considered a decision-making process and a method for discovery, which is always done for a purpose that varies from study to study (Elliot, 2018). For the present study, the coding consisted of two rounds during which we individually coded the data using the following questions:

1 Why did the experts develop the cybersecurity in-service training in the way they did from the point of view of customers' learning (that is, improving competencies)?

2 How did the experts' perceptions of the qualities that improved customers' competencies match with Herrington et al. (2010) attributes of an authentic learning environment (considering also the elements that the experts mentioned that did not match those of Herrington et al., 2010) and elements which these three scholars identified but the in-service training did not introduce)?

Between the individual coding rounds, we had a meeting to discuss the findings and made small amendments to the second coding question.

During this meeting, we also agreed to reduce the number of interviews from five to four, as one of the interviewees was newly appointed to his position and had considerably less experience in designing and conducting in-service training than the others. His responses to the interview questions often started with sentences such as: 'well, I do not have experience of this issue, but …', which indicated a lack of expert knowledge.

All the specialists emphasised that optimal in-service training should offer the opportunity to experience or immerse oneself in a situation and event; which should reflect and correspond to real-life situations in the participants' work. For example, one specialist stated that the environment does not need to be an exact copy of real life; however, it must be 'sufficient for the learner to throw him/herself into the situation as if he/she was really experiencing it at work'. Thus, we turned our focus to how the environment and the in-service training could be made sufficiently realistic to adequately correspond to real-life situations. In other words, we analysed which elements the specialists spoke about as being sufficiently realistic and the crucial elements for ensuring individual and organisational learning for complex real-life situations to ensure the maintenance of business process performance in cases of cyber interference. Several previous studies examined and utilised technical competence frameworks, such as NICE, for cybersecurity training (Campbell et al., 2015; Jacob et al., 2018; Paulsen et al., 2012). Due to the limited focus on the human factors (Lehto et al., 2017) or social layers (Dawson and Thomson, 2018) of cybersecurity, we decided to focus in more detail on these aspects of the data, which will become apparent in the lower-level categorisations.

We applied a rather conventional qualitative content analysis (Drisko and Maschi, 2016; Hsieh and Shannon, 2005) as an analytical technique to sort the coded data into categories and to achieve a higher level of interpretation, involving merged categories and eventually themes. Each category consisted of groups of codes that seemed to refer to the same issue on a level of 'what is visible and obvious in the data', whereas themes were the underlying meanings and answers that overlapped all the categories on the latent level [Erlingsson and Brysiewicz, (2017), p.94]. Our approach was abductive (Graneheim et al., 2017), combining inductive and deductive approaches. In the present study, this meant that our analysis was data-driven; however, we also utilised the concepts of Herrington et al. (2010) in our coding to reflect on the perceptions of the experts, and eventually moved back and forth between the data and the theory to create a more complete understanding of the phenomenon and to strengthen our interpretation of the data.

4 Results

Our analysis identified three fundamental components that were omnipresent when maintaining cybersecurity for business processes, since cybersecurity always takes place in a digital environment. Moreover, cybersecurity is never conducted alone when

ensuring business process performance (Dawson and Thomson, 2018): it always involves team collaboration, and the team very often includes personnel from different levels or functions of an organisation, or even from different organisations. At the very least, a network of collaborators or customers needs to be informed in the case of a cybersecurity incident. Furthermore, due to the environments in which business processes encounter cybersecurity threats, complexity is always apparent (Karjalainen and Kokkonen, 2020; Karjalainen et al., 2019). By this we mean that different hardware and software technologies and networks combined with different consumers, users, organisations, policies, and motivations for actions permeate the whole environment, making causal connections difficult to predict and foresee:

> "Services today are quite extensive and complex, and they are not single points inside the business; they are really large packages that involve a wide variety of components, and those different components produce the company's services and products. So, if the attack focuses on the service of one company, as usually happens, the other actors [partners, subcontractors, service providers] have to be involved in managing the situation. We are also able to perform and practice partner networking with our clients … After all, they are all customers and they are all involved in the exercise, but therefore act like participating organisations … when participating in the exercise. In a way, we are able to produce a whole scenario that they should understand, and for them information is formed, such as ways of operating and doing and controlling that scenario. What is the role of the service provider in the security of the service owner's service, for example?"

We named these fundamental components the *technology layer*, *human layer* and *complexity layer*, which were the three themes that permeated all the categories, (i.e., the elements that an optimal in-service training environment should include to ensure appropriate training of individuals and organisations in the competencies required for dealing with real-life cybersecurity incidents) and ensuring the maintenance of business process performance.

Before forming higher-level categories, we identified eight different categories of elements in the data, which referred to training in:

- the technical environment where the business processes and cyber incidents take place and appropriate solutions
- the various functionalities of an organisation
- the process of interpretation
- chains of commands, and roles and responsibilities
- social trust and teamwork among groups of people
- public relations
- inter-team communication (how to conduct a risk analysis including cause–consequence analysis)
- the formulation of inter-team conceptions that they can share (often with personnel from different organisations)

The first two items included several other sub-categories; however, these aspects were thoroughly covered in previous studies (Damodaran and Couretas, 2015; Pham et al.,

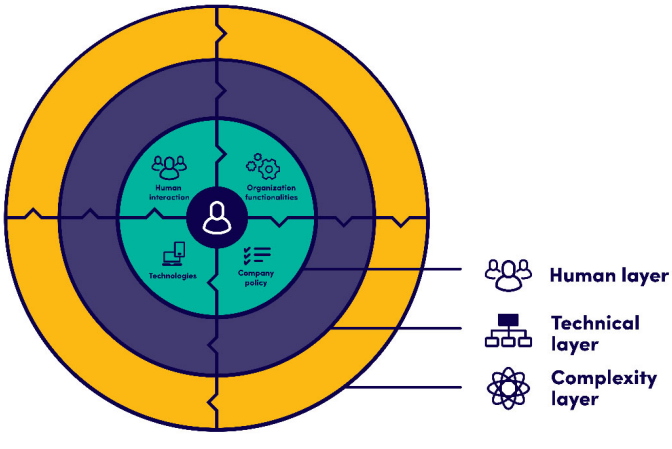
2016; Vykopal et al., 2017), and we therefore focused on the other aspects in the present study.

All these elements are related to the needs of customers and learners. This meant that the real-life effect and efficiency of the exercise depended on co-design with the customer to support the needs of the organisation, as became apparent, for example, in the next interview extract:

> "Exercise models and activities are built that way because the goal is to develop the organisation. In a way, you don't aim to train individuals separately, but that's how you do it: it reflects how the organisation works, and you can develop the organisation's ability to work and find solutions. People who participate in exercise are not necessarily so widespread in the organisation or within the customer. So, the organisations development targets will come up during the exercise, even when you don't know before the exercise what they are; that's how it works and you build the reason for the exercise and development with the customer. For some clients who have done the exercises more often, it is easier because they have a routine to follow. It is more challenging for first-timers to figure out what they should do and what they aspire to practice. They don't know how to practice, and they have to understand the practice in terms of the bigger picture. But they come to understand what you want to focus on because, in a way, the big picture is constructed from the small details and they understand that you can't practice all the details in one exercise."

Based on these eight elements, we analysed and formulated four higher-level categories: *technologies*, *human interaction*, *organisational functionalities*, and *company policies*. The elements are presented in Figure 1.

Figure 1 The components and categories for optimal in-service cybersecurity exercise (see online version for colours)



Next, we will explain these categories before considering the findings in light of authentic learning theory.

4.1 Technologies

The technical environment that should be learned and mastered is a complex entity with different layers. Instead of being an isolated technology environment, the cybersecurity

specialists perceived it as only one component of a business process, as the following extract shows:

> "When we think about the business, we discover that it has changed, and we know the role of IT has changed over the past decade quite significantly from a supporting role to the core of the business. IT enables so many things for the business today. It is one thing to be able to run the services, but to do it in a secure and reliable way is quite another. And this has caused an issue: when companies are analysing risks, they discover that, today, most of the risks for businesses come from digital environments."

The different layers to be mastered and learned are, for example, the technical environment that the end user (learner) has to be able to configure and manage and the technical infrastructure that the end user (learner) cannot influence directly. The first includes, for example, end devices or terminals, the administrative and production systems used by the company, the company servers, the company communication network, firewalls, and other internet access services. The latter consists, for example, of the internet network topology, internet services, and cloud services. Depending on the learning objective, in an advanced cyber arena-style (Karjalainen and Kokkonen 2020) learning environment, the learner can be assigned a role or task to enable him/her to practice all the mentioned technical layers and thus increase his/her own understanding of organisations technical entity. The learner uses technology to detect cybersecurity threats and learns how the threats manifest in different technologies, how to trace a threat actor, and how to block a threat actor's activities using technologies. It is also important to be able to demonstrate for the learner the limitations and implications of technology on different layers.

4.2 Organisational functionalities

The second category in which learning in practice was pursued focused on the various functionalities of an organisation. It could be said that the technical level produces cybersecurity phenomena, and the risks of those phenomena need to be managed, mitigated, or eliminated by the various functionalities built into the organisation. This means, for example, the maintenance of administrative and/or production systems through various processes, which may be internal company processes or extend to the company's customers, partners, or the subcontracting chain, as became apparent in the next interview extract:

> "When we talk about the big companies, or when the company is more like a traditional industry company, it is obvious that the whole production of the company will cease if the IT systems are not functioning: nothing will happen if IT stops functioning. If you experience a disruption of the logistics chain run by the business's partners, it will affect the factory's production and the factory will not produce anything beyond that point, because they will have no raw material to do anything with."

Depending on a company's industry, specific incident response processes can be built into the organisation to manage vulnerabilities and events caused by cyber threats. Such industries include, for example, internet providers, banks, and large industrial operators. Regarding smaller companies, it is often the responsibility of a partner organisation to produce and maintain digital service platforms, which brings about a need to understand and manage operational processes across organisational boundaries.

Communication has become increasingly important with the expansion of social media use. Often, the exercise aims to increase understanding of and action regarding, for example, technical system operators, decision-makers, and communication actors. This takes us to the third level of learning in a cybersecurity exercise – human interaction.

4.3 Company policies

This category covers the perceptions of the cybersecurity experts regarding the different norms, regulations, and obligations that the organisations used to guide and manage their operations. In the present data, these were related to the chains of commands in the organisation and to guidelines concerning public relations:

> "Well, this is the 'glue' of our exercise activities; that we study existing models and try to train on them, and measure them, together with the customer. If they do not have models to work with, we have at least researched it and can provide open material about the current, standard, or de-facto way of doing things. On the other hand, when we simulate a cyber phenomenon in a model – a sufficiently well-modelled environment for a customer – the customer works around that cyber phenomenon and can act in the same way he/she would in real life, when this happens, or if it happens … Then in real life, when something does happen, he/she has some experience and a model that he/she can then refer to and start acting on. Capability improves when a situation is not new."

Maintaining guidelines and policies is often resource-intensive, and a rapidly changing operating environment creates challenges for the maintenance of up-to-date guidelines and policies. Sometimes, the changed operating environment shapes the organisation's work practices, which drift away from the guidelines and policies. Such a situation should be detectable, since doing things in violation of the guidelines over a long period affects the organisation's operating culture and activities; the existing guidelines and policies are not followed because they are not up to date. A cyber security exercise is a good tool for benchmarking and measuring an organisation's ability to act according to instructions, verify the timeliness of instructions, and identify possible needs for updates.

4.4 Human interaction

This higher-level category included the cybersecurity experts' perceptions of the communication inside the organisation, their interpretations of what counts as an incident, their understanding of incidents as situations that have to be responded to and how to do this, and their reflections on team spirit and trust. For an organisation to be able to function and understand the activities of its various components or departments, people working in the organisation must be able to communicate work issues to other groups of employees in the organisation, facilitating risk analysis and promoting social trust among members of the group. These dimensions of a cybersecurity exercise were referred to in the following interview:

> "There are [in the exercise] completely non-technical people, administrative people, and technical specialists, which causes challenges for the focus on the exercise. What challenges are likely to occur in the exercise? Well, this possibly does not answer the question, but I'll still say that one of the major challenges in organisations is that the different kinds of actor's don't have a common language to communicate. When we speak about these cyber-attacks

> and … overall, about IT and technical details, if they are involved in the business and the organisation's different activities … the problems are, how to form a common understanding and what kind of terminology people will use. People tend to use jargon if they work as business directors or in public relations, in IT, or in security; they all use different jargon, or it might be that the same term has different meanings for the different actors … so misunderstanding easily occurs. So, this is something that we always have to consider in the exercise … My opinion is that this will always happen, so people need to understand each other and agree on how to communicate. The exercise is also helpful for training in communication … so, in that sense, many people understand it wrongly by thinking that these exercises are only technical exercises. In fact, during the exercise, you diverge from the technical level and focus mostly on human interactions between people."

The ability of technical personnel to effectively communicate vulnerabilities or risks in a technical operating environment to the personnel dealing with the business operations of an organisation is important. The technical staff should be able to understand how technical vulnerabilities affect the business. A risk management process makes it easy to handle this problem. When a technical person encounters a technical vulnerability in their own operating environment that should be corrected, they should be able to communicate the technical measures for its mitigation or elimination and the potential costs involved. If, within his or her own remit, the technical person is unable to eliminate the vulnerability or mitigate the risk to a tolerable level, he/she should communicate the risk to his/her supervisor. During this interaction, it is important to be able to communicate the risk and its effective severity so that the supervisor is able to prioritise the risk and allocate the necessary corrective actions and resources to mitigate or eliminate the risk. If the supervisor's own authority or resources are not sufficient, he/she should communicate the risk further within the organisation. The organisation's risk management process then manages the identified risk by mitigating or eliminating it, or making a decision to tolerate the identified risk and manage it through certain control measures.

For the process described above to work seamlessly, a common and consistent language and culture within the organisation is required to collectively determine, for example, the impact of a risk on business continuity, its management, or the methods and resources necessary to eliminate the risk. The example described above refers to the technical ability to identify a vulnerability or cybersecurity event that has occurred, the event or incident management process, the risk management process, and the other management process. Practicing a common organisational language, interpreting causal relationships, understanding roles and responsibilities, and building trust and community spirit are the key goals of learning in cybersecurity exercises. Practicing the various human activities described above can also extend to the interaction between stakeholders outside the organisation, such as communicating with customers, service providers, or the subcontracting chain.

4.5 The findings and the authentic learning theory

Herrington and Oliver's (2000) nine requirements for an authentic learning environment that simulates a real operating environment are relevant and current in light of the present study. The interviewed experts emphasised an adequately authentic context, which sufficiently corresponds to the way the knowledge and skills are used when cybersecurity incidents occur. The experts considered simulation a multidisciplinary process that is

important for acting in real-life situations. Thus, in addition to the activities being authentic, the in-service training should sufficiently simulate the whole process of acting so that different roles and collaborative knowledge-sharing and creation occur naturally in the learning process.

In their guide to authentic e-learning, Herrington et al. (2010) discussed and articulated how to foster personal ownership of learning. Disparate viewpoints create cognitive conflicts, which challenge understanding. However, what appears to be important in the context of professional cybersecurity is that speaking and articulating are means to convey and interpret information and decide whether an incident requires a reaction. Cybersecurity incidents are, by nature, not always very straightforward, and the environment is very complex, which is why cybersecurity experts have to be able to identify different incidents and conduct their risk analysis efficiently, not only individually, but together with their peers. In other words, they have to be able to communicate successfully to and with their team about the possible threats; what actions and strategies may be needed, why, and who is responsible; and what consequences the threats, different actions, and strategies may have. The team may include personnel with different backgrounds, native languages, and fields of expertise, which underlines the importance of solid discussion and reflection and is why conscious pauses for reflection (Herrington et al., 2010) are also an important part of cybersecurity exercises. Articulating, reflecting on, and taking responsibility for communication are not solely matters of learning but are inseparable parts of efficient professional cybersecurity.

An authentic context extends beyond examples from real working life. Herrington et al. (2010, pp.17–18) stated that 'the context needs to be all-embracing, to provide the purpose and motivation for learning, and to provide a sustained and complex learning environment that can be explored at length'. The present study demonstrated that a sufficiently authentic cybersecurity context necessarily includes a digital environment that is complex and allows collaboration to take place. In addition to these fundamental components, the authentic context should include opportunities to learn about techniques and technologies, organisational capabilities, human interaction, and company policies. Without these aspects, there is a high risk of over-simplification, which Herrington et al. (2010) recommended avoiding. They pointed out that the complexity of the learning environment should be aligned with the final performance environment and that simplifying learning contexts does not enhance learning.

5 Conclusions

The present study examined the requirements for optimal in-service cybersecurity training by focusing on the various aspects of cybersecurity exercises that will guarantee the maintenance of business process performance if cybersecurity incidents occur. The approach was qualitative and relied on content analysis methods (Drisco and Marschi, 2016; Hsieh and Shannon, 2005).

We identified three fundamental components – a *technology layer*, a *human layer*, and a *complexity layer* – as themes that cover all the elements that an optimal in-service training environment should contain to train individuals and organisations in the competencies they will need for dealing with real-life cybersecurity incidents and ensure the maintenance of business process performance. These components were identified not only from the data but also from previous studies, which perceived human cooperation

during cyber incidents as essential (Dawson and Thomson, 2018) and complexity as an essential part of the environment in which cybersecurity and business processes operate (Karjalainen and Kokkonen, 2020; Karjalainen et al., 2019).

The elements that we identified were *technologies* that should be learned and mastered in a complex entity with different technical layers; *organisational functionalities*, referring to the various functionalities, (e.g., subcontracting chains) that are built into an organisation; *company policies* that normalise and regulate a company's operations; and *human interaction*, which includes several aspects of people working together in and between organisations. These findings contribute to the previous studies on cyber exercises (Brilingaitė et al., 2020; Karjalainen and Kokkonen, 2020; Karjalainen et al., 2019) by illuminating and explicating the requirements for realism in the exercise context.

Contributing to the studies on simulation pedagogy (Lathleiff, 2019; Rystedt et al., 2019), the present study points out that, by taking part as an organisation (rather than individually) and by practicing the whole action process (rather than only some situations or examples), processes can be properly managed to ensure that business performance is maintained following a real-life cybersecurity incident. This involves including all important parts of the process, including the technical environment and solutions, the functionalities of an organisation, effective risk analysis, real roles and responsibilities, the group of people normally working together, and communication between organisations and their partners as parts of the in-service training. In this way, the whole process of acting when a cybersecurity incident occurs can be simulated in an exercise.

The findings were highly aligned with pedagogical theories on authentic learning environments (Herrington and Oliver, 2000; Herrington et al., 2010). Built on these findings, this paper recommends that cybersecurity professionals should have an overall understanding of the operating environment and should be able to develop their own skills in response to operating environment changes. It is also important to be able to tie one's own cyber knowledge into the frame of reference of the operating environment (business, etc.). Cybersecurity is not implemented for its own sake, but as part of a diverse business environment. Deep technical expertise must be integrated into a business entity to facilitate understanding of the complex effects of the IT operating environment as part of the business. This raises new challenges for both the content of teaching and the demands of teaching environments. Cyber security exercise environments have sought to meet these requirements.

The present study also shows that cybersecurity as a phenomenon combines the digital and physical worlds, and both of these should be included in the educational environment. The learning environment should thus embody individual security controls, the technical cybersecurity architecture, and manifestations in the physical environment, such as human interaction, organisational functionalities, structures, and instructions. According to Parrish et al. (2018), this field is multifaceted, and our study illuminates the elements that should be included when cyber exercises are used as a pedagogical method for in-service training. However, we also consider these elements to be important learning content for degree studies.

The sample of experts from only one organisation was a limitation for the study, since the results were based on the experiences and perceptions of a rather homogeneous group. However, we were aware that these experts had varied work backgrounds, (e.g., in the Finnish Defence Forces and in private sector cybersecurity companies). They had also

experienced several international cybersecurity exercises, such as the NATO Cyber Coalition and NATO Locked Shields exercises, and we thus considered them to have sufficient understanding of the requirements for optimal in-service training implementation.

This comprehensive incorporation of the complexity of the operating environment makes us question whether a cyber arena-style environment is the only appropriate environment for organising in-service training, in which all the essential competencies needed to maintain business processes if a cyber incident occurs must be considered and developed. At least the cyber arena style environment allows for training in genuine work skills in an environment that corresponds to the real environment. Moreover, the elements identified as important in cybersecurity training (see Figure 1) may be equally important in more generally in ICT teaching. The main phenomenon of the digital age is the digitalisation of technology and business, which is leading to increasing numbers of so-called traditional business fields not thought of as IT operating environments needing IT knowledge and skills. Thus, the elements presented might also be generalised to training in industries operating with the support of information systems or other digital operating environments.

As the present study showed, the capability to solve complex problems in collaboration with a multi-disciplinary group of professionals has become one of the most important requirements for educational environments (Dawson and Thomson, 2018; Parrish et al., 2018). To contribute to the growing need for heutagogical learning abilities, which embrace self-determined learning motivation and competency development (Canning, 2010; Hase, 2009) we encourage future research to explore solutions for comprehensive learning environments with online or remote access. These solutions would increase the possibilities for continuous learning throughout professional cybersecurity careers.

References

Amis, J. (2005) 'Interviewing for case study research', in Andrews, D.L., Mason, D.S. and Silk, M.L. (Eds.): *Qualitative Methods in Sports Studies*, pp.104–138, Berg, New York.

Bariran, S., Sahari, K. and Yunus, B. (2013) 'A novel interactive OBE approach in SCM pedagogy using beer game simulation theory', *International Journal of Asian Social Science*, Vol. 3, No. 9, pp.2034–2040.

Berman, S.J. (2012) 'Digital transformation: opportunities to create new business models', *Strategy and Leadership*, Vol. 40, No. 2, pp.16–24.

Brilingaitė, A., Bukauskas, L. and Juozapavičius, A. (2020) 'A framework for competence development and assessment in hybrid cybersecurity exercises', *Computers and Security*, Vol. 88, https:doi.org/10.1016/j.cose.2019.101607.

Campbell, S.G., O'Rourke, P. and Bunting, M.F. (2015) 'Identifying dimensions of cyber aptitude: the design of the cyber aptitude and talent assessment', in *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, Vol. 59, No. 1, pp.721–725, SAGE Publications, Sage CA, Los Angeles, CA.

Canning, N. (2010) 'Playing with heutagogy: exploring strategies to empower mature learners in higher education', *Journal of Further and Higher Education*, Vol. 34, No. 1, pp.59–71.

Damodaran, S.K. and Couretas, J.M. (2015) 'Cyber modeling and simulation for cyber-range events', in *Proceedings of the Conference on Summer Computer Simulation*, July, pp.1–8.

Dawson, J. and Thomson, R. (2018) 'The future cybersecurity workforce: going beyond technical skills for successful cyber performance', *Frontiers in Psychology*, Vol. 9, DOI: 10.3389/fpsyg.2018.00744.

Drisko, J.W. and Maschi, T. (2016) *Content Analysis*, Oxford University Press, New York.

Elliot, V. (2018) 'Thinking about the coding process in qualitative data analysis', *The Qualitative Report*, Vol. 23, No. 11, pp.2850–2861.

Emin-Martinez, V. and Ney, M. (2013) 'Supporting teachers in the process of adoption of game based learning pedagogy', in *ECGBL 2013 – Proceedings of the European Conference on Games Based Learning*, Porto, Portugal, October, pp.156–162.

Endicott-Popovsky, B.E. and Popovsky, V.M. (2014) 'Application of pedagogical fundamentals for the holistic development of cybersecurity professionals', *ACM Inroads*, Vol. 5, No. 1, pp.57–68.

Enescu, S. (2019) 'The concept of cybersecurity culture', in *The Fourth Annual Conference of the National Defence College Romania in the New International Security Dynamics*, Carol I National Defence University Publishing House, pp.176–191.

Engestrom, Y. (2001) 'Expansive learning at work: toward an activity theoretical reconceptualization', *Journal of Education and Work*, Vol. 14, No. 1, pp.133–156.

Ericsson, A.K. (2008) 'Deliberate practice and acquisition of expert performance: a general overview', *Academic Emergency Medicine*, Vol. 15, No. 11, pp.988–994.

Erlingsson, C. and Brysiewicz, P. (2017) 'A hands-on guide to doing content analysis', *African Journal of Emergency Medicine*, Vol. 7, No. 3, pp.93–99.

European Commission (2013) *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.2.2013 JOIN (2013) 1 final.

Gantzias, G. (2020) 'Dynamics of public interest in artificial intelligence: business intelligence culture and global regulation in the digital era', in *The Palgrave Handbook of Corporate Sustainability in the Digital Era*, pp.259–281, Palgrave Macmillan, Cham.

Graneheim, U.H., Lindgren, B-M. and Lundman, B. (2017) 'Methodological challenges in qualitative content analysis: a discussion paper', *Nurse Education Today*, Vol. 56, No. 2, pp.29–34.

Guild, E., Carrera, S. and Geyer, F. (2008) *The Commission's New Border Package: Does it take us one Step Closer to a 'Cyber-Fortress Europe*?, CEPS Policy Brief No. 154, March [online] https://ssrn.com/abstract=1334058 or http://dx.doi.org/10.2139/ssrn.1334058 (accessed 23 November 2020).

Hammer, M. and Champy, J. (1993) *Re-engineering the Corporation: A Manifesto for Business Revolution*, Harper Business, New York.

Hase, S. (2009) 'Heutagogy and e-learning in the workplace: some challenges and opportunities', *Impact: Journal of Applied Research in Workplace E-Learning*, Vol. 1, No. 1, pp.43–52.

Hatfield, J.M. (2018) 'Social engineering in cyber security: the evolution of a concept', *Computers and Security*, Vol. 73, pp.102–113, ISSN: 0167-4048.

Herrington, J. and Oliver, R. (2000) 'An instructional design framework for authentic learning environments', *Educational Technology Research and Development*, Vol. 48, No. 3, pp.23–48.

Herrington, J., Reeves, T.C. and Oliver, R. (2010) *A Guide to Authentic E-Learning*, Routledge, New York.

Hsieh, H.F. and Shannon, S.E. (2005) 'Three approaches to qualitative content analysis', *Qualitative Health Research*, Vol. 15, No. 9, pp.1277–1288.

Jacob, J., Wei, W., Sha, K., Davari, S. and Yang, T.A. (2018) 'Is the nice cybersecurity workforce framework (NCWF) effective for a workforce comprised of interdisciplinary majors?' in *Proceedings of the International Conference on Scientific Computing (CSC)*, pp.124–130, The Steering Committee of the World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Kalaniti, K. and Campbell, D.M. (2015) 'Simulation-based medical education: time for a pedagogical shift', *Indian Pediatrics*, Vol. 52, No. 1, pp.41–45.

Karjalainen, M. and Kokkonen, T. (2020) 'Comprehensive cyber arena; the next generation cyber range', in *Proceedings of 2020 IEEE European Symposium on Security and Privacy Workshops, EUROS&PW 2020*, Institute of Electrical and Electronics Engineers IEEE, pp.11–16.

Karjalainen, M., Kokkonen, T. and Puuska, S. (2019) 'Pedagogical aspects of cybersecurity exercises', in *Proceedings of the 4th IEEE European Symposium on Security and Privacy Workshops, EUROS&PW 2019*, Institute of Electrical and Electronics Engineers IEEE, pp.103–108.

Kolb, D.A., Boyatzis, R.E. and Mainemelis, C. (2001) 'Experiential learning theory: previous research and new directions', in Zhang, L. (Ed.): *Perspectives on Thinking, Learning, and Cognitive Styles*, pp.227–247, Lawrence Erlbaum Associates, Mahwah.

Kong, Y., Kayumova, L. and Zakirova, V.G. (2017) 'Simulation technologies in preparing teachers to deal with risks', *Eurasia Journal of Mathematics, Science and Technology Education*, Vol. 13, No. 8, pp.4753–4763.

Kucek, S. and Leitner, M. (2020) 'Training the human-in-the-loop in industrial cyber ranges', in *Digital Transformation in Semiconductor Manufacturing*, pp.107–118, Springer, Cham.

Kurniawati, E., Siddiq, A. and Huda, I. (2020) 'E-commerce opportunities in the 4.0 era innovative entrepreneurship management development', *Polish Journal of Management Studies*, Vol. 21, No. 1, pp.199–210.

Larrucea, X. and Santamaría, I. (2020) 'Designing a cyber range exercise for educational purposes', in Yilmaz, M., Niemann, J., Clarke, P. and Messnarz, R. (Eds.): *Systems, Software and Services Process Improvement, EuroSPI 2020, Communications in Computer and Information Science*, Springer, Cham, Vol. 1251.

Lathleiff, C. (2019) *Imagining an Authentic Workplace using Simulation: Exploring Simulation Pedagogy in Auditing Education*, Unpublished PhD thesis, University of Kwazulu-Natal.

Lehto, M., Limnéll, J., Innola, E., Pöyhönen, J. Rusi, T. and Salminen, M. (2017) *Suomen kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi [Finland's Cybersecurity: The Present State, Vision and the Actions Needed to Achieve the Vision]*, Publications of the Government´s analysis, assessment and research activities 30/2017, Prime Minister´s Office, Finland.

Lindsay, A., Downs, D. and Lunn, K. (2003) 'Business processes – attempts to find a definition', *Information and Software Technology*, Vol. 45, No. 15, pp.1015–1019.

Lupovici, A. (2011) 'Cyber warfare and deterrence: trends and challenges in research', *Military and Strategic Affairs*, Vol. 3, No. 3, pp.49–62.

Maennel, K. (2020) 'Learning analytics perspective: evidencing learning from digital datasets in cybersecurity exercises', in *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, pp.27–36.

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, Portland OR.

Ministry of Defence Finland (2019) *EDA Cyber Ranges Federation Project Showcased at Demo Exercise in Finland* [online] https://www.defmin.fi/en/frontpage/topical/press_releases/2019/eda_cyber_ranges_federation_project_showcased_at_demo_exercise_in_finland.10065.news#2dcffe66 (accessed 23 November 2020).

Mouheb, D., Abbas, S. and Merabti, M. (2019) 'Cybersecurity curriculum design: a survey', in Pan, Z., Cheok, A., Müller, W., Zhang, M., El Rhalibi, A. and Kifayat, K. (Eds.): *Transactions on Edutainment XV. Lecture Notes in Computer Science*, Vol. 11345, pp.93–107, Springer, Berlin, Heidelberg.

Nystrom, S., Dahlberg, J., Edelbring, S., Hult, H. and Dahlgren, M. (2016) 'Debriefing practices in interprofessional simulation with students: a sociomaterial perspective', *BMC Medical Education*, Vol. 16, p.148, https://doi.org/10.1186/s12909-016-0666-5.

Parrish, A., Impagliazzo, J., Raj, R.K., Santos, H., Asghar, M.R., Jøsang, A., Pereira, T. and Stavrou, E. (2018) 'Global perspectives on cybersecurity education for 2030: a case for a meta-discipline', in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, pp.36–54.

Paulsen, C., McDuffie, E., Newhouse, W. and Toth, P. (2012) 'NICE: creating a cybersecurity workforce and aware public', *IEEE Security and Privacy*, Vol. 10. No. 3, pp.76–79.

Petersen, R., Santos, D., Wetzel, K., Smith, M. and Witte, G. (2020) *Workforce Framework for Cybersecurity (NICE Framework)*, National Institute of Standards and Technology, U.S. Department of Commerce.

Pham, C., Tang, D., Chinen, K.I. and Beuran, R. (2016) 'Cyris: a cyber range instantiation system for facilitating security training', in *Proceedings of the Seventh Symposium on Information and Communication Technology*, December, pp.251–258.

Rashid, N.A., Bin Othman, Z., Bin Johan, R. and Sidek, S.B.H. (2019) 'Cisco packet tracer simulation as effective pedagogy in computer networking course', *International Journal of Interactive Mobile Technologies*, Vol. 13, No. 10, pp.4–18.

Rystedt, H., Dahlgren, M.A., Felländer-Tsai, L. and Nyström, S. (2019) 'Advancing simulation pedagogy and research', in Abrandt Dahlgren, M., Rystedt, H., Felländer-Tsai, L. and Nyström, S. (Eds.): *Interprofessional Simulation in HealthCare*, pp.197–211, Springer, Cham.

Saharinen, K., Karjalainen, M. and Kokkonen, T. (2019) 'A design model for a degree programme in cybersecurity', in *Proceedings of 11th International Conference on Education Technology and Computers*, Association for Computing Machinery, New York, NY, pp.3–7.

Schon, D.A. (1987) *Educating the Reflective Practitioner*, Jossey-Bass, San Francisco.

Secretariat of the Security Committee (2013) *Finland's Cybersecurity Strategy, Government Resolution 24.1.2013* [online] https://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf (accessed 23 November 2020).

Sisaneci, I., Akin, O., Karaman, M. and Saglam, M. (2013) 'A novel concept for cybersecurity: institutional cybersecurity', Paper presented at the *6th International Conference on Information Security and Cryptology*, Turkey, Ankara, 20–21 September.

Švábenský, V., Vykopal, J., Cermak, M. and Laštovička, M. (2018) 'Enhancing cybersecurity skills by creating serious games', in *Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, pp.194–199.

The NATO Cooperative Cyber Defence Centre of Excellence Exercises (2019) [online] https://ccdcoe:org/exercises/ (accessed 19 February 2019).

Tian, Z., Cui, Y., An, L., Su, S., Yin, X., Yin, L and Cui, X. (2018) 'A real-time correlation of host-level events in cyber range service for a smart campus', *IEEE Access*, Vol. 6, spp.35355–35364, DOI: 10.1109/ACCESS.2018.2846590.

Uckan Farnman, B., Koraeus, M. and Backman, S. (2015) *The 2015 Report on National and International Cybersecurity Exercises: Survey, Analysis and Recommendations*, Technical Report, Swedish Defence University, CRISMART, National Center for Crisis Management Research and Training [online] https://www:enisa:europa:eu/publications/latest-report-on-national-and-international-cyber-security-exercises (accessed 20 August 2020).

Von Solms, R. and Van Niekerk, J. (2013) 'From information security to cybersecurity', *Computers and Security*, Vol. 38, pp.97–102, ISSN: 0167-4048.

Vykopal, J., Vizváry, M., Oslejsek, R., Celeda, P. and Tovarnak, D. (2017, October) 'Lessons learned from complex hands-on defence exercises in a cyber range', in *2017 IEEE Frontiers in Education Conference (FIE)*, pp.1–8.

Winter, H. (2012) 'System security assessment using a cyber range'. Paper presented at the *7th IET International Conference on System Safety, incorporating the Cybersecurity Conference*, 15–18 October.

Yamin, M.M., Katt, B. and Gkioulos, V. (2020) 'Cyber ranges and security testbeds: scenarios, functions, tools and architecture', *Computers and Security*, Vol. 88, pp.101–636, ISSN: 0167-4048.

Appendix

The first part of the interview

Introductory questions:

- Tell me about yourself, who are you, where you come from, and how you came to work in this organisation.
- Why do you think you were selected to participate in this interview?

Questions relating to the background of the informant:

- Could you tell me about your experience of developing cybersecurity in-service training environments (cyber arenas)?
- If you were to describe to an ordinary person like me, who has no idea about cybersecurity, how the training environment works and logic underpins it, what would you say?
- What kinds of exercises are arranged within such an environment?

Questions relating to learners and users of the training environment:

- What kind of learners are the environment designed to serve?
- For what kind of learners does it work best, and why?
- What exercises are normally organised in the training environment?
- What is your own role in those exercises and in the development and maintenance of the environment?
- Which role do you personally find to be the most motivating with respect to the environment?
- Do the clients/learners have certain qualities or attributes that you have to pay attention to when you design in-service training practices or exercises for them?

Questions relating to the functionality and use of the training environment and exercises/in-service training:

- How did you decide on the particular logic of the exercises for the in-service training? Why do they run as they run?
- What kind of learning activities or processes do the exercises or in-service trainings serve best?
    a If the informant does not talk about this, ask a follow-up question: How do the exercises or in-service training allow for learning in teams?

- If you were to describe the process of learning that the exercises or in-service training facilitate, what would it be like?
- What qualities of cyber security exercises especially facilitate learning?
- How do you ensure that the exercises or in-service trainings are up-to-date?
- How is the learning reflected during the exercises or in-service trainings?
- How do you guide participants during the practice activities?
- If you had a magic wand and you could change anything about the environment, the exercises, or the overall in-service training, what would you change and why?

The second part of the interview

Please consider one-by-one the items shown on the slides:

- How does the environment and the in-service training take account of this issue?
- Could something be improved from this point of view?
    1 An authentic context that describes or corresponds to the way in which knowledge and skills are used in real life.
    2 Authentic activities that reflect the main content of the whole course or study unit.
    3 Learners are provided with models of how to actually act in real-life situations.
    4 Learners are enabled and encouraged to take on different roles and consider their learning and the environment from different perspectives.
    5 Opportunities are provided for collaborative knowledge creation.
    6 Opportunities are provided for learners to reflect on their levels of competence and learning relative to the context of the learning environment, authentic tasks, and expertise.
    7 Opportunities are provided for students to articulate and justify their actions and choices to others.
    8 Students are provided with community support for the learning process that does not oversimplify the learning environment but prepares and creates support structures for them to do things in a meaningful way.
    9 Assessment of learning that is tightly integrated into activities, allowing learners to focus on activities and learning and to produce products and outputs in collaboration with others.