International Journal of Adult Education and Technology
Volume 14 • Issue 1

Learn to Train Like You Fight

Mika Karjalainen, Independent Researcher, Finland*
Anna-Liisa Ojala, Independent Researcher, Finland
Marko Vatanen, Independent Researcher, Finland
Jarno Lötjönen, Independent Researcher, Finland

ABSTRACT

This qualitative study includes nine semi-structured interviews with cybersecurity experts from different security-related organizations who are familiar with cybersecurity exercises. Its contribution to cybersecurity workforce development focuses on organizational learning rather than individual skills development and relevant competencies. It was found that the utilization of thematic analysis methods develop individual readiness and expertise. It also enhances the maturity of an organization's processes, roles, communication, and exercise capabilities. Moreover, the exercises increase social trust between individuals and organizations through business-to-business cooperation. However, there were several barriers and challenges in utilizing learned skills and competencies within an organization, including a need to increase the capacity of staff members who participate in the exercise.

KEYWORDS

Continuous Education, Cyber Arena, Cyber Exercise, Cyber Range, Cyber Security, Cyber Security Education, In-Service Training, Organizational Learning, Pedagogy, Training

INTRODUCTION

Do Cybersecurity Exercises Benefit an Individual or Organizational Learning?

Maersk, the world's largest shipping container company, faced a cyberattack in 2017. According to some estimates, a Maersk ship, which can carry up to 20,000 containers as once, will port somewhere across the globe every 15 minutes (Walton, 2022). On this day, the cyberattack forced Maersk to shut down all operations, costing the company $250 million and $300 million. Companies down the supply chain also lost millions of dollars due to this cybersecurity incident (Capano, 2021).

This case is just one example of the current business reality in which almost all companies have built their processes and operations on digital information systems. Like Maersk, companies face vulnerabilities as systems interface with digital systems that are operated or used by other organizations.

In the digital era, businesses rely on information systems to serve as a platform and core of business operations. The vulnerabilities typical to digital systems also apply to many nations' critical

DOI: 10.4018/IJAET.322085 *Corresponding Author

infrastructures and operations. Information and communication technologies (ICTs) serve as an enabler of modern society's business operations, which can challenge organizations due to their rapid digital advancements. It is, therefore, crucial for organizations to keep pace with technological developments and exploit new technologies while managing threats. Organizations must manage their own environment and the effects of the network due to the highly networked ecosystem structure. Cybersecurity professionals must be able to manage a complex environment that includes evolving technologies, internal and external processes within the organization, and human interactions (Lindsay et al., 2003).

Organizations should focus on continuous skills and knowledge development to adapt to an ever-changing environment. Team members must be diligent and reactive in their response to internal and external triggers (Luecke, 2003). The development of individual competencies should also transfer into the organization's capabilities. In changing digital environments that face threats, organizations cannot simply react to real-time change. Instead, they must actively increase their capacities to predict the need for capacity development within their teams.

Prior research explored the development of individual competencies through cybersecurity exercises (e.g., Ferguson et al., 2014; Karjalainen & Ojala, 2022; Pham et al., 2016; Vykopal et al., 2017). However, there is a lack of knowledge on the impact of cybersecurity exercises on organizational learning or an understanding of the features and mechanisms that enhance or hinder organizational learning. This deficiency underlines the rationality of the present study. The resource-intensive exercises should urge participating organizations to ask questions about the extent to which the competence development of individuals is turned into the competence of the organization. Subsequently, organizations should question the processes or features that hinder or advance organizational learning.

Argyris (2002) defined organizational learning as "a process of detecting and correcting error" and error as "any feature of knowledge or knowing that inhibits learning" (p. 116). In other words, in this approach, organizational learning is not an accumulation of knowledge. Instead, it occurs when barriers that hinder learning are identified and removed. The organizational learning process also requires changes in organizational knowledge (Schulz, 2017). Revisions are needed in practices and ways of thinking that impact the performance of the organization (Chiva et al., 2014).

In the process of learning, the mismatch diminishes between actual and intended actions. The actions are more likely to have intended consequences (Argyris, 2002). Robinson (2002) emphasized the problem-solving aspect of the process of organizational learning. Her study used universities and their problem-solving practices in student recruitment and enrollment efforts to show how organizations depend on their capacities and capabilities to solve problems and improve practices.

Finally, during the organizational learning process, organizations must adapt to their environments (Huber & Glick, 1993). In doing so, they must actively develop and respond to environments that support their successful performance (Robinson, 2001).

These approaches are important for cybersecurity-related issues in organizations. Organizations solve many problems related to cyberthreats or, as in the present study, problems related to the competence development of a workforce. Organizations must adapt to, create, and respond to environments in which the threats take place. They must also pay attention to environments in which they collaborate with other organizations. Furthermore, organizations must manage processes of knowledge accumulation and processes of detecting and correcting errors.

The present study examines organizational learning processes in the context of cybersecurity exercises. This is achieved by examining how the participants perceived the exercises as a means and opportunity to revise processes like knowledge management and problem solving. Organizations must develop working environments that support organizational maturity in cybersecurity.

This issue is examined with three research questions:

1. Whose actions or knowledge changes due to cybersecurity exercises. How do they change?
2. What challenges do the participants experience when putting what they have learned into practice within their organizations?

3. Are there cybersecurity-related features in the exercises that appear to support or challenge organizational knowledge creation?

The first two questions guide the composition of the semi-structured interview questions. The analysis was inductive. The third question was created after becoming more acquainted with the data and exposing the results of the first two questions about organizational learning theories.

The researchers found that the organizational knowledge creation process is essential for organizations that send their personnel to commercial training to become more competent in facing cyber incidents. In organizational knowledge creation, individuals' tacit knowledge is transferred into explicit knowledge. It is then turned into the tacit knowledge of an organization (e.g., Basten & Haamann, 2018; Martínez & Ruiz, 2006; Nonaka, 1994; Nonaka & Konno, 1998). Furthermore, by exposing the results to conceptions of single- and double-loop learning (Argyris, 2002, 2004; Argyris & Schön, 1978, 1996), it was noted that organizational learning in cybersecurity exercises is structured with laws and company policies that set the framework for organizational development.

After introducing the context and theoretical background of the study, this article presents the qualitative methodology and thematic analysis. The results section corresponds to the research questions. The first two research questions are organized around thematic analysis. The third research question is ordered according to secondary analysis and organizational theories. The discussion recaps the key results and presents the implications of the study.

CYBERSECURITY AND EXERCISES

The term "cybersecurity" has been established over the last two decades (Enescu, 2019; Hatfield, 2018; Warner, 2012). There are several definitions for cybersecurity. The most frequently used definition describes cybersecurity as an expansion of the traditional definition of information security (safeguarding the accuracy, integrity, and usability of data).

In addition to information security, digital systems are affected by (or through) the physical world (Von Solms & van Niekerk, 2013). The digital operating environment is characterized by its continuous expansion and transformation. This, combined with the integration of the digital operating environment and physical world, makes its complexity a special feature of the cybersecurity environment (Sinha, 2014; Törngren & Grogan, 2018). Complexity challenges the controllability of the environment and the capacity to operate in it, teach it, and learn the cause-and-effect relationships of related entities (Karjalainen et al., 2019; Moser & Cohen, 2013; Skirpan, 2018; Švábenský, 2020). The cybersecurity operating environment combines elements of different technical entities. Teaching these competencies and skills places special demands on the teaching environment, which is often described as a cyber range or cyber arena (Ferguson et al., 2014; Karjalainen & Kokkonen, 2020; Pham et al., 2016; Vykopal et al., 2017).

There are several distinctive means of organizing cybersecurity workforce development. Cheung et al. (2012) considered cybersecurity competitions to offer limited support for competence development, suggesting that hands-on learning methodologies are more efficient. Many contemporary cybersecurity courses include hands-on tasks, even when organized online (O'Connor & Stricklan, 2021). The most comprehensive cybersecurity exercises simulate tasks faced by the workforce on a regular basis (Karjalainen et al., 2019). These exercises may have a competitive element if employees compete against other teams on cybersecurity assignments (e.g., Kim et al., 2019).

The participants in the present study engaged in a realistic simulation of real-life work with sufficiently realistic teams. Instead of competing against each other, the team members partnered to solve real-life problems and enhance their collaborative competence development. The partnerships, interfacing systems, and real-life problems increased the complexity of the exercises, bringing team members closer to complexities faced by experts in their regular work (Karjalainen, 2021).

The effectiveness of these cybersecurity exercises has been studied, especially from the perspective of learning technical elements (Chapman et al., 2017; Frank et al., 2017; Liu et al., 2019). Research has expanded in recent years to depict a more holistic view of the learning environment and aspects of cybersecurity (Brilingaitė et al., 2020; Karjalainen, 2021; Karjalainen & Kokkonen, 2020, Leitner et al., 2021; Maennel, 2020; Yamin & Katt, 2022).

The present study expands the understanding of previous studies by examining the possible transfer of individual competencies learned at a cybersecurity exercise to the overall competencies of organizations. Organizational competencies and the mechanisms of their development have also been studied previously (e.g., Drejer, 2000; Murray & Donegan, 2003). However, there is a lack of research that connects the development of organizational knowledge to the context of cybersecurity although cybersecurity training is a significant economic investment for organizations that seek to develop their competencies by sending their workforce to the exercises.

Theoretical Background

To explain and structure the findings, the first two research questions—theories on organizational trust (e.g., Aydan & Kaya, 2018; Wilson & Nielson, 2001; Zhao et al., 2021) and job satisfaction (Bakker, 2011)—were utilized together with theories on organizational processes (Henkel et al., 2019; Metz, 2021; Schweiger et al., 2018) and simulation training (Nestel et al., 2018). However, further analysis produced a question about the features in the exercises that appear to support or challenge organizational knowledge creation. Thus, it produced a need for the third research question and a deeper exploration of theories related to organizational learning. In particular, the researchers drew on the theory of single- and double-loop learning developed by Argyris and Schön (1978, 1996; also, Argyris, 2002) and organizational knowledge creation theory by Nonaka (1991; also, Nonaka & Konno, 1998). Despite these theories being developed decades ago, they are still relevant and acknowledged approaches in organizational learning studies (Basten & Haamann, 2018).

Single-loop learning occurs when an error is corrected, but the values and policies behind it remain untouched. In double-loop learning, the values and practices behind the error are changed with the error's correction (Argyris, 2004; Argyris & Schön, 1996). Single-loop learning describes a situation in which an organizational member detects an error in the organization's operations and reacts to the error by correcting it in a way that preserves the attributes that enable the error to occur, such as design guidelines, processes, or governing regulations. In double-loop learning, a member of the organization corrects the error while ensuring that the root cause that enabled the error is found and corrected so the error does not recur in the future. In doing so, the organization can learn from the mistakes and correct and improve its performance.

Organizational learning depends strongly on individuals acquiring knowledge and skills that guide them in changing their behavior. Organizational knowledge is based on an individual's experiences, contacts, or attitudes, which are then processed into new knowledge and skills (Kolb et al., 2001). The spiral of organizational knowledge creation is based on the concept of tacit and explicit knowledge (Nonaka, 1994). According to Polanyi (1966), explicit knowledge is knowledge that can be shared through formal systems or spoken information. On the other hand, tacit knowledge is an understanding that is known to the individual, typically through experience. It is difficult to share formally through a system of communication. Typically, tacit knowledge is formed experientially, whereas explicit knowledge is often oriented toward past events without a specific context (Nonaka & Takeuchi, 1995).

According to Nonaka and Takeuchi (1995), organizational knowledge is created in four ways: (1) socialization; (2) externalization; (3) integration; and (4) internalization. Socialization allows tacit knowledge to be transferred between individuals or from an individual to a group. The process of externalization can be described as the communication or documentation of tacit knowledge. In integration, explicit knowledge existing in individuals is combined through the social process, for example, by speaking. The process of internalization is understood as the assimilation of explicit knowledge into an individual's personal tacit knowledge (Nonaka, 1994).

METHODS

It is necessary to capture rich data on how participants of cybersecurity in-service exercises experience the learning needs, training, and outcomes in the capacity development processes of their organizations. This supports the study of how participants in cybersecurity exercises experience the ability to transfer knowledge and skills that are co-created, shared, and produced in exercises to the day-to-day practices of their working organizations.

The researchers decided to collect this data using semi-structured interviews. In past years, this method was been identified as an atypical method to collecting research data in engineering sciences (Howe & Anda, 2005). It has become more popular among technologically oriented studies (e.g., Dadzie et al., 2018; Richter et al., 2016). Semi-structured interviews were suited to the present study because the researchers were interested in hearing the independent thoughts of the informants. It was also thought that they might have valuable insights beyond the researchers' structured interview questionnaires (Adams, 2015).

However, organizations and their cybersecurity teams are not eager to produce data or help scholars publish public studies on their approaches, activities, or processes. Thus, gaining access to this research site was more challenging than with topics not related to security (e.g., Amis, 2005). At the beginning of a one-week cybersecurity exercise, the researchers contacted management-level participants and asked whether they and their organization would be willing to join a short interview during the week. Participants had the opportunity to express willingness, decline, or ask for consent from their organization before and after the interview.

The researchers were able to gain consent from nine participants from different security-related organizations with whom interviews were conducted during the week. Security-related organizations actively train their team members, which is why they were selected. Some of these organizations were smaller in terms of their staff force; some had several hundred members. Not all the staff members were cybersecurity experts. In many of these organizations, cybersecurity was one aspect of their expertise. The researchers agreed with the organizations that this is all they would tell about them and their staff.

The interviews lasted from 16 to 36 minutes. They took place in a meeting room in which each question was displayed on a screen and read aloud. After each participant provided their personal information and history in the field, the recordings began. The following questions were asked:

- How many times have you taken part in cybersecurity exercises and in which positions?
- How do you find these exercises to be different from taking part in courses, if at all?
- How are these exercises able to support learning in the topics or tasks of the exercises?
- Have the exercises and analysis built on the exercises produced concrete actions at your organization and, if so, what kind?
- Do you find the final analysis of the exercise helpful in supporting the learned issues in becoming part of the daily processes of your organization?
- If you think about the previous exercises, have you found the roles at the organizations (or positions) taking part in the training adequate?
- Can you identify actions in the training that would support either the exercise or the day-to-day practices of your organization to become more valuable for your organization?

Follow-up questions were also added, if necessary. The participants were asked to extend their responses beyond the questions when needed. All the informants and organizations trusted that the researchers would carefully reconsider what kind of interview examples can be published and what was only helpful for the analysis. There were some moments during which the informants told the researchers to close the recording because of sensitive information. These cases reminded the scholars that the interview information was a gift from the organizations and, thus, cannot be used carelessly.

The interviews were transcribed. All parts that were considered professionally too sensitive to were removed from storage. There were two coding rounds for the data (Amis, 2005). Answers were marked related to the following questions:

1. Whose practices are experienced to be changed and how?
2. What kinds of challenges exist in utilizing and transferring the learned practices (processes, competencies, practices, approaches, and skills) to the day-to-day practices of the organization?

After both rounds, a meeting was held to discuss the findings and the experiences of the quality of the data with respect to the research questions.

The researchers found the data to be sufficient for answering the questions. This was a welcome realization due to challenges in persuading participants to take part in studies of security-related organizations. Both analysis rounds produced matrices on the findings, including examples of the data and several remarks on the findings. The findings were read together with theories that further explained the themes that had been created and elaborated upon. Thereafter, the themes were cross-read with theories on organizational learning (Aydan & Kaya, 2018; Bakker, 2011; Henkel et al., 2019; Metz, 2021; Schweiger et al., 2018; Wilson & Nielson, 2001; Zhao et al., 2021).

Basten and Haamann's (2018) literature review was utilized, as well as the theoretical backgrounds of previous studies (e.g., Antunes & Pinhero, 2020; Bontis et al., 2002; Engström & Käkelä, 2019; Martínez & Ruiz, 2006), to further examine if certain cybersecurity-related features appeared to support or challenge organizational knowledge creation related to these exercise periods. This phase of the study was surprisingly time-consuming because the data appeared to be significantly more complex than the organizational learning models. Combining ideas on single-loop learning, double-loop learning (Argyris 2002; Argyris & Schön, 1996), and the knowledge creation of organizations as a dynamic process (Nonaka, 1991; Nonaka & Konno, 1998) offered a sufficient theoretical framework to explain what features should be highlighted when ensuring that organizational learning is associated with cybersecurity training practices.

RESULTS

The findings of the study are presented in three sub-sections. The first presents whose actions are experienced to be changed and in what ways due to cybersecurity exercises. The second shows what kinds of challenges the participants experienced in putting the learned into practice after cybersecurity exercises. The third concentrates on the features that appear to support or challenge organizational learning related to cybersecurity exercises.

Organizational Maturity Increases by Exercising

Using thematic analysis, the study identified four categories to describe the experiences of the participants whose actions changed and the ways in which they changed: (1) individual readiness and expertise increased and has been tested; (2) the maturity of an organization has increased in processes, roles, communication, and exercise capability; (3) social trust between individuals and trust toward organizations has increased; and (4) business-to-business cooperation has increased and has been enhanced.

Individual Readiness and Expertise Increases and Is Tested

This category includes all the notions related to individual competence development — the experiences of advancing individual learning processes (Kolb, 1984). The participants were able to learn new skills or apply old ones in new ways during the exercises. Their understanding of actions and consequences increased, and they were able to test their individual skills.

The participants felt that they increased their personal knowledge and skills (for example, participating in exercises on rare cases of cybersecurity attacks or with cases they could not practice in day-to-day work). It was also a safe environment to allow incidents to develop further than normal because they could observe the consequences of these diverse types of incidents. For example, one participant felt it worthwhile to gain experience with what happens if there is malicious software on the computer:

We know there is an infected computer. We can follow lateral movements or see if it exfilters something from there or somewhere else. By doing so, we can get a wider picture of the operation or threat actor…with composure, we can benefit more in the bigger picture and in real life through this exercise.

The participants also valued the possibility of safely becoming acquainted with working in their discomfort zone:

The crisis situation teaches that in real life there is no possibility to train [for] the crisis when it takes place. There are situations in which you must drag on or extend to the extreme. These exercises have taught, for example, that people will find their places.

The moment of crisis is too occupied and stressful for any organization to allow practice. Thus, it is worthwhile to have safe environments to expose employees to pressures and feelings of discomfort while still performing and following the same roles and processes that should be followed in real life. Additionally, the participants felt they had been able to apply skills that were learned in other contexts, such as courses or work, and were able to test those skills and tools that could be useful in their real role.

Testing individual skills may not be a key aim of the exercise, especially if considered to be outside control. Some participants mentioned that the exercise can be a tool for checking "how [a] worker [in] his team performed at the exercise." One participant, for example, explained that the exercise is used to teach newcomers to follow the right processes:

We have this situation where almost all our staff members are now first-timers at this exercise. I've noticed that they take shortcuts in the processes and have some idea that this is how it's always done … they think why should I contact the Security Operation Center, for example? And you see that they have this particular thing [approach/way of acting] and now we have to try and all learn to use the right process models. And when we leave these exercises, we of course emphasize this still.

As becomes apparent in the interview extract, these exercises are also used for testing how team members work individually and together with respect to company policies and procedures. The other side of the same issue was the increased understanding of participants' capacity with respect to the organization and wider context of different collaborators, which was also mentioned in the interviews. These findings align with experiential learning theories (e.g., Kolb, 1984). However, the present study focuses on organizational learning. Thus, elaboration on the different aspects of individual learning is not mentioned here.

Maturity of an Organization Increases in Processes, Roles, Communication, and Training

Organizational maturity refers to the organization's capabilities regarding a certain discipline (Rosemann & de Bruin, 2005). In this category, the notions of increased maturity become apparent in the participants' comments. First, they explain their experiences surrounding clarified, practiced, and tested processes, procedures, and divisions of labor in the working roles of the organization. Second, they discuss how the staff learns and which media they use to communicate with one another.

Third, they explain how their learning allows them toa better utilize the different expertise areas of the personnel as they perform and communicate at the intersection of technological expertise and non-technological expertise. Fourth, their explanations explore how the organizations have improved their exercise and development maturity by increasing their exercise motivation by identifying processes, conventions, and lack of competencies that should be changed or improved.

One participant, for example, described how their organization utilized the exercise to pilot their processes, procedures, and cooperation with other organizations.

Our aim has been to help people in this field get to know each other within our organization…to consolidate and test if the procedures and processes that we have described and documented are functional. This kind of exercise supports proceedings, which, of course, include cooperation with other organizations. So, this exercise is, I think, a fine opportunity to pilot those described and documented processes that we have. And the background and different roles of the crew will support how the procedures will be examined from different points of view and reflected in their role and expertise.

As explained, cybersecurity is managed by many organizations. They must find the right persons and tools for communication to ensure that the information is shared as needed.

Most of the interviews noted that the exercise supported maturity, readiness to train, and eagerness to develop within in the organization:

Let's say we can react to these issues in advance because we have been at these exercises. These analyses and actions of putting these to practice have led to situations in which we have done our own smaller-scale exercises.

Furthermore, the organizations identified the parts of processes and facilities that are crucial for high-quality performance and development.

What may be one of the biggest challenges for us, which we have also acknowledged during these exercises, [is] we have an urgent need for internal domestic networking. We have the need, but we don't have a platform for it…but the need is now identified.

After this statement, the participant explained that there are many ways of doing activities within a nationwide organization even if these activities should be standardized with respect to terms of classification and law. The exercises have improved networking. They have also indicated the urgent need to adapt.

Identifying activities, processes, and lack of competencies provides a concrete mandate to suggest change. The exercise also works as a quality assurance tool for the operational staff to identify needs for development and gain reinforcement for these arguments.

Social Trust Between Individuals and Organizations Increases

On the one hand, the present study views social trust as socially constructed reliability built on social processes and structures. On the other hand, social capital becomes embodied in networks that can be utilized as resources like the need for information (e.g., Anheier & Kendall, 2002). Both forms of social trust were identified in the interview data. One participant depicted the exercises from a social point of view:

We utilize this exercise for getting to know other people because we don't actually [meet] every day. There are individuals who we know are related to cybersecurity issues, but we rarely connect or meet. So, we bring these people together and it opens communication channels for our daily work. It also enhances collaboration.

As the participant described, the exercises bring people together, generating cooperation and common understanding. These team members also form networks that can be utilized if cooperation is needed to solve problems.

In addition to trust between individuals, trust in their organizations became apparent. Participants expressed delight at the contribution the training made to advance change within their organizations. "We can say that some have even smiled when they noticed that their feedback was taken advantage of," one participant said when he described the effects of the exercise on his organization. Thus, participants expressed organizational trust based on positive experiences and expectations about the intent and behavior of their team members (Shockley-Zalabak et al., 2000). The notion of smiling indicates that this trust also increases job satisfaction, Previous studies have reported that trust in managers and colleagues is a significant predictor of job satisfaction (Sarıkaya & Kara, 2020).

Business-to-Business Cooperation Increases

Like networking between individuals, business-to-business cooperation includes networking between organizations. According to studies by Wilson and Nielson (2001) and Heide and Miner (1992), these contain dimensions of information sharing, organizational flexibility in case of changed circumstances, harmony to allow bilateral cooperation and tools in governance mechanisms, and collaboration to advance joint or reciprocal decision-making and problem-solving processes. Trust between organizations is also a result of cooperation, serving as a key factor in successful relationship building (Wilson & Nielson, 2001). These dimensions were found in the data, as becomes apparent in the following interview extract:

We trained here together…we did not, for example, understand why we should inform the National Cyber Security Center. Reporting an incident was something we did not want to do because we were afraid of a loss in reputation. We did not, for example, know that the National Cyber Security Center is a reliable agent that acts as part of the reliable network. They can help in different situations. So, we changed our processes and will inform them now. How it took place was that they introduced themselves to us here and told us that they are a reliable agent.

Due to the exercise, information was shared, flexibility and adaptations were shown, harmony in terms of governance mechanisms increased, and joint work was advanced. The notion of trust includes the idea of allowing oneself to show vulnerability, uncertainty, doubt, or dependency. This also became apparent in the example.

Scholars who examine the healthcare sector have reported that trust is a key factor in promoting a willingness to report on negative situations and incidents at work (e.g., Aydan & Kaya, 2018; Zhao et al., 2021). Additionally, the previous informant reported concerns related to a loss of reputation in cases of cyber incidents. However, because of the exercise, trust between organizations has increased and advanced the error reporting processes.

Barriers Experienced That Inhibit Learning of Organizations

The challenges experienced in utilizing learned skills and competencies (or reacting to insufficiencies in the processes) were related to inadequate preparation, challenges in focusing on the training, challenges of communication, or issues in participation, reflection, and managerial acts.

Participant Roles are Insufficient for Fulfilling the Objectives of the Organization

The cybersecurity exercise was a simulation of real working life. According to the data, this is also the approach the participants take when engaging in the exercise. It is like taking part in a role-playing game that imitates the day-to-day practices of the participating organizations. However, it is a closed network with incidents that occur in a significantly more frequent manner compared to real life.

According to Nestel et al. (2018), realism in learning simulation is as fruitless as the possibility of always defining what is real in the present world. To support optimal learning, they do not aim to focus on defining what needs to be real, when, and for whom. Instead, they suggest there should be a shift in focus from realism to meaningfulness. Meaningfulness is an individual perception. As the present data explicates, although organizations set their learning objectives for the cybersecurity exercise, the participants they sent to the exercise did not always cover the roles that would be needed for simulating the real working environment in a meaningful manner. The following extract depicts the experience of a participant:

I've observed this game for a week. I've noticed that at the designing phase, we should change the way that we would involve more SOC [Security Operation Center] people, NOC [Network Operation Center], and monitoring-related things. Maybe we didn't think so technically [of] them. We have to have some communications specialists or communications side specialists who know how to fix e-mails … or a LYNC [Microsoft Lync] specialist. That is, maybe we would not need so many technical experts in specific fields here.

It could be deduced that the more realistic the training team is, the better the participants can recognize the effect of distinct roles on the successful execution of real-world operations and processes. One participant remarked that if at least one management-level person participated in the training, they would not have to "make up" how to act in situations in which they contact management. Thus, if the participating team does not sufficiently reflect the roles of real life, it can be challenging to meet the learning objectives during and after the exercise.

Managerial Support for Conducting Change Is Incomplete

Two key findings related to this category were apparent in the data. First, the participants felt that managers lacked exercise experience and built their understanding on textual reports. These managers did not actively take part in the exercise days; hence, they lacked an awareness and comprehension of the need for change. Due to inactive participation, conclusions and proposals for operations were also based on a textual end report, which lacked the dimension of experience. These reports are not always shared within the organization. Second, a lack of clear steps and leadership for change was experienced after the exercise. The participants also experienced a lack of commitment from leadership to support effective change. One informant explained:

Quite often, the remarks from here would be taken to them [work]. In our case, we talk about norms, regulations, orders, and guidelines [at work]…we would take the remarks to those [to our organization]…we would take the pieces and the reason behind it…like, is it lack of documentation or lack of guidelines or something. Partly, it gets better all the time, but I still see that we would need more support from the management.

According to Gill (2003), management's commitment to change becomes visible through a willingness to invest resources, an awareness of the impact of their behavior, and regular reviews of progress. Change management does not necessarily refer to major change processes of an organization. It can also refer to the "adoption of an idea, procedure, process, or behavior that is new to an organization" (Metz, 2021, p. 612), which is the case of the changes in the present data and previous example. Typically, there is also resistance to change in an organization (e.g., Schweiger et al., 2018). In the case of these exercises, the employees appear to be agile and proactive to adapt to change. However, they do not receive adequate support for implementing change in the organization.

As the previous informant explained, the preparations for these exercise weeks take several dozens of hours for each participating organization. The week itself takes another 30 hours for each participant. There is clear pressure from the managerial side to get back to regular work after the exercise week. Again, this hinders the possibility of carrying out the process before and during the

exercise. In other words, management offers support and resources for development and learning, but the final support for implementing change is considered incomplete.

However, some participants were critical of how well the management level understands the processes and threats related to cybersecurity:

Do they [managers] see the threat [as] what would happen if, for example, information from personal ID cards or [the] passport system was suddenly presented on a cover page of some yellow magazine? Can they really understand the threats as they exist in the current world?

The support of management for the required change would be that the managers would participate in the exercise, which was suggested by many participants in the present data.

Inter-Organizational Processes Challenge Change

Inter-organizational processes often take place where complex services or products are developed or delivered (Henkel et al., 2019). Cybersecurity processes are examples of processes that require a network of interconnected organizations and phases to deliver products (in this case, supporting cybersecurity for the business processes of an organization). These inter-organizational processes challenge changes to other processes, as studies have stated (Breu et al., 2013). This also becomes apparent in the present data, as the following interview extract displays:

If we notice something related to one organization, making this change to the whole chain is challenging. I mean, if it is in our feed and in the other organization's feed…all start to report on the same feed…there is more pressure, and we might get it changed.

One informant also described a case in which there was a need to make changes to another organization's processes, which was significantly challenging.

According to Henkel et al. (2019), inter-organizational collaboration is typically noted by studies in three forms: (1) products being exchanged; (2) processes that cross organizational boundaries; and (3) processes for which several organizations contribute with assets or resources. Inter-organizational collaboration in cybersecurity-related processes can represent any of these forms, which creates challenges for changes in these processes.

"Real Work" Does not Enable Optimal Training

The exercise aims to improve the capacity and prowess of the participating organization and its staff. However, it separates the staff from productive work on exercise days:

We have a positive problem in our hands: the [number] of exercises is increasing. This causes pressure for us as an operative organization because we cannot attach all professionals or operative workers to all exercises…it would cause insecurities for our operative work. We can't afford to do so.

This also causes the problem that "more staff members are asked to participate in exercises and to be trained," as another participant explained. Some participants felt that there should more exercises and more rotation of participants from their organizations.

The data showed that participants who engaged in regular work tasks felt it interfered with their concentration on the exercise:

When the lessons can be learned here at the exercise, we accomplish some sharing of knowledge… we must consciously keep the working computers away so that we can concentrate on the exercise and conduct those tasks.

Moreover, some participants felt that the exercise could be considered distinct from real day-to-day work and life may continue as it was after the exercise:

It is so that when Monday comes, you are there. Do you have more time to invest after that? You would need as many hours as you've used for preparing to take the perceptions and notes back to the daily norms.

These extracts show the complexities of continuous competence development within organization's workforce.

Orientation to the Exercise in Insufficient and Participants Focus on Wrong Issues

As explained, simulation training is a simulation of real-life work. It is organized to emulate real actions and processes in a sufficient, meaningful (but not necessarily fully realistic) manner (Nestel et al., 2018). However, these simulations are not real workdays during which team members solve their real-work problems. Additionally, these exercises have distinct objectives for real workdays. That is, they aim to develop capacities and processes. Hence, there is no need for the exercise environment to be complete. It should be simply sufficient and meaningfully realistic. Some processes or incidents can be observed without action (unlike day-to-day work). The data showed that this is not a problem for participants who have taken part in previous exercises. However, newcomers may find it a challenge if the orientation to the exercise has not been adequate.

Individual practitioners should understand their role while taking part in this exercise and training. When the basic cyber expert takes part in this exercise, the other [first] starts to make the exercise environment more difficult because it's "cool" to do so and they want to make it harder for the opponent to act. We must always tell them that this is not the aim…if we had the patience, we could get a bigger picture and more advantages in real life through this exercise.

It can be interpreted that the orientation does not support the newcomer's adoption and understanding of the aims of the exercise. It also shows that the identity of a cybersecurity expert, including their actions, is so strong that adopting a new approach takes time.

One participant mentioned that they had problems convincing their team members that taking part was safe and that they would "lose" in the exercise. Many cybersecurity exercises are organized in a competition format in which organizations compete against each other. The aim is to win. During their internal orientation, this organization was convinced that the format was aimed at learning and improving processes and collaboration. Thus, the participants should not "play against the game, but observe and communicate."

Barriers to Communication Between Technical Personnel and Management

Participants experienced barriers to effective communication between technical personnel and management regarding the threats or non-functionalities of the technical level identified in the exercise. This impacted learning and change in organizations:

We need to be able to talk through from that point of view…we don't bring technology or technical vocabulary to the managers. Instead, we bring the consequences of actions. There should be a person who can whisper to the other side that this technical issue means "this." And this should be documented.

Communication barriers between technical personnel and management in technology-related organizations are not novel issues. They were reported by Utterback (1971) regarding the effectiveness

of companies in originating, developing, and implementing technical innovation. Killingsworth and Jones (1989) used the concept of specialized discourse communities when speaking about specialized language practices that involve distinct terminology and jargon related to divisions of labor, professions, topics, tasks, and skills. These specialized discourse communities use, share, and cherish distinct conceptions of their work-related communication.

As the previous interview extract depicted, cybersecurity experts and managers operate in different discourse communities. Thus, there may be barriers to communication. In this way, managing cybersecurity also becomes about managing communication within organizations (see also Karjalainen & Ojala, 2022).

ORGANIZATIONS DEVELOP CYBER MATURITY THROUGH ORGANIZATIONAL LEARNING

It can be observed from the first research question that the exercise helps to reflect on and improve organizational processes with respect to cybersecurity. These processes are acts during which staff members solve cybersecurity-related problems faced during their regular work tasks (cf. Robinson, 2001). Improvement requires adaptation (Huber & Glick, 1993), reaction, and active development of the environments that support successful performances with collaborators (Robinson, 2001). Effective and reliable processes, as well as the policies guiding them, are critical for efficient cybersecurity.

However, the findings related to these improved processes were difficult to set to the theoretical framework of single- and double-loop learning (Argyris, 2002; Argyris & Schön, 1996). Some situations and processes described by participants were guided by laws (e.g., a report of an offense) or company policies (e.g., technical solutions or cooperation networks the organization uses or is contracted to use). In other words, double-loop learning, during which norms and values are reconsidered, may have several obstacles in security-related organizations and cybersecurity processes. However, Robinson (2014) argued that revising governing variables is not always necessary. Plus, single-loop learning can be sufficient for many occasions.

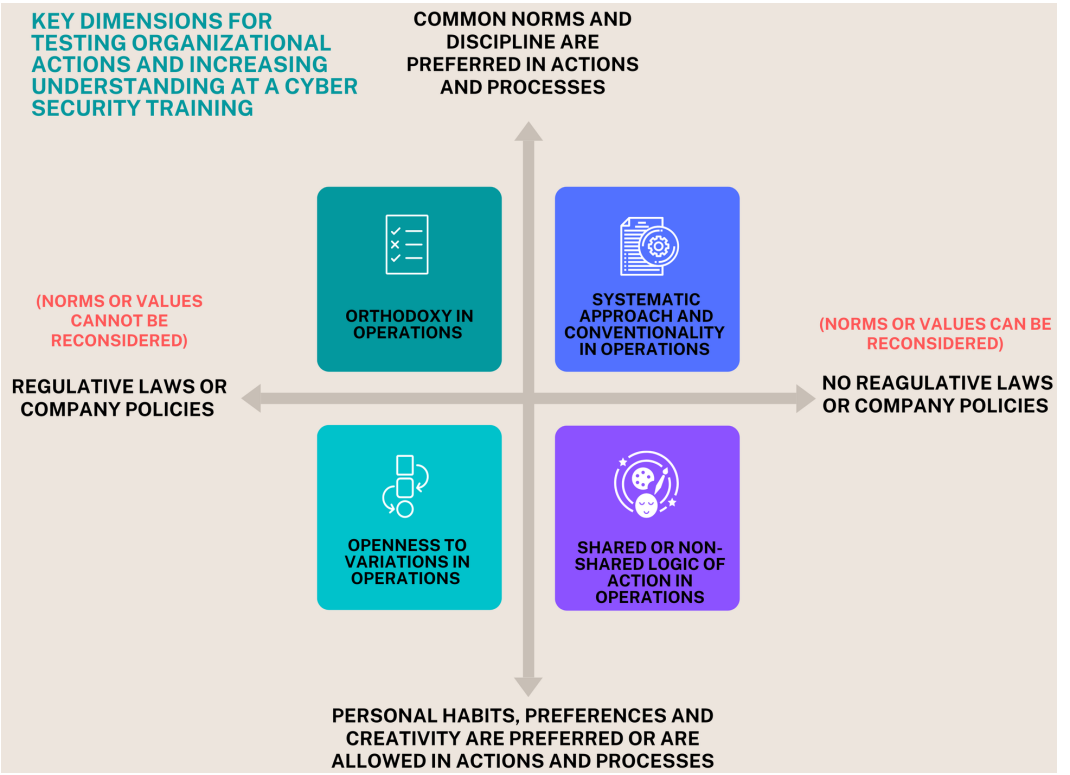
It can be observed that organizations or teams may want everyone to follow a specific order, norm, or uniform chain of actions. With some processes, however, uniform ways of acting are not critical. It is known from previous studies on work psychology that the possibility of personal job crafting may increase job satisfaction and work engagement (Bakker, 2011). So, not every task should be guided by norms, which would "specify how things should be done" (Scott, 2013, p. 64) during a working day. With the results of the present study, it can be acknowledged that organizational work crafting, during which the whole team crafts processes and problem-solving mechanisms are improved and clarified, increases job satisfaction and work engagement (see Figure 1).

The left side of the figure represents actions and processes of cybersecurity that are regulated by laws or company policies. The right side illustrates actions and processes with no laws or company policies regulated. The upper section depicts preferred actions and processes to follow norms and discipline. The actions and processes of the lower section of the four squares promote personal habits, preferences, and creativity.

The participants valued the networks that they created with employees of their own and coordinating organizations. They could personally utilize these relationships when needed (for example, to ask a second opinion). These actions or processes do not have to be guided by norms. However, in the case of cyber threats, personnel must know which laws and policies to follow and how the team is expected to act or cooperate with other organizations. These processes must be shared and well-practiced. Organizations must be agile in deploying and developing these processes when pressured with cyber-incident situations.

With the second research question, it was noticed that learning in organizations is challenged by issues related to the exercise (e.g., inadequate roles or regular tasks that interfere with concentration on the exercise) and problems related to how the organization functions (e.g., communication challenges

Figure 1.



between technical personnel and management). The participating team of the organization could reconsider some values and norms or consider which processes should be changed per the double-loop learning (Argyris, 2002). However, this would still not ensure organizational learning. The knowledge should be shared with and managed by the management whose support is needed to ensure the change.

During the phases of socialization, externalization, and combination, knowledge is shared with individuals who take part in the exercise. Tacit knowledge is translated into words, terms, visuals, and other forms that can be understood by other members who take part in the exercise. Later, this knowledge is disseminated to and reflected on by other groups within and outside the exercise. If the exercise reaches these stages, it will still require the internalization phase to ensure organizational knowledge creation and learning (Basten & Haamann, 2018; Nonaka & Konno, 1998).

The internalization phase transforms this knowledge into the organization's tacit knowledge. According to this study, many cybersecurity-related processes mingle or are shared with other organizations' processes. Thus, the actions leading to change would require support from the management of both organizations. According to the findings, there may be a lack of managerial support for conducting inter-organizational changes. If the processes are intertwined with the processes of collaborative organizations, organizational learning takes place, and change can be noticed only at the knowledge level, but it never reaches the action level.

CONCLUSION

The present study examined organizational learning processes in the context of cybersecurity exercises. First, it examined how actions and/or knowledge changed due to practice. Second, it studied the

challenges experienced by participants when putting the learned material into organizational practice. Third, it explored whether cybersecurity-related features in the exercises supported or challenged the creation of organizational knowledge.

The qualitative study was built on nine semi-structured interviews. Representatives from security-related organizations took part in cybersecurity exercises and organizational learning theories (Argyris, 2002, 2004; Argyris & Schön, 1978, 1996; Basten & Haamann, 2018; Martínez & Ruiz, 2006; Nonaka, 1994; Nonaka & Konno, 1998).

Like previous studies (Karjalainen & Ojala, 2022), the current study demonstrated that technical skills and maturity are a small part of cybersecurity competence development in the workplace. The study contributes to the existing literature on cybersecurity workforce development (e.g., Brilingaitė et al., 2020; Karjalainen, 2021; Leitner et al., 2021; Maennel, 2020; Vykopal et al., 2017; Yamin & Katt, 2022) by focusing on organizational learning rather than individual skills development and competencies. The exercises developed individual readiness and expertise. They also increased maturity within an organization's processes, roles, communication, and capabilities. In addition, it increased social trust between individuals and organizations, enhancing business-to-business cooperation.

There were several challenges in utilizing the learned skills and competencies for the sake of the whole organization or increasing the capacity of the staff who participated in the exercise. These barriers were related to inadequate preparation and communication, difficulties in focusing on the training, and issues regarding participation, reflection, and managerial acts. If the participating team does not sufficiently reflect on real-life roles, it could be challenging to meet the learning objectives during and after the exercises. Furthermore, the participants felt that managers lacked exercise experience, built their understanding on textual reports, and demonstrated limited commitment and leadership to lead change. There were also barriers to communication between technical personnel and management. Additionally, intertwining processes with other organizations challenged organizational learning because making changes to another organization's processes was viewed as significantly challenging. Sometimes, the regular work tasks did not enable optimal training or orientation to the exercise, which directed the participants' focus to incorrect issues.

The third research question was created after exposing the results of the first two research questions to organizational learning theories. Organizational learning in cybersecurity exercises is structured with laws and company policies that set the framework for organizational development. This affects opportunities to aim at or prefer single- or double-loop learning (Argyris, 2002, 2004; Argyris & Schön, 1978, 1996) in several processes and skills. However, Robinson (2014) pointed out that revising governing variables is not always necessary and single-loop learning can be sufficient for many occasions. Key dimensions were suggested for testing organizational actions and increasing the understanding of cybersecurity exercises. The first dimension was regulative laws and company policies; the second was common norms and discipline in actions and processes. The exercise appeared to be a good environment for organizations to explore the situations and processes that must be followed, are preferred shared norms and discipline to be followed, are open to variations, or follow personal preferences. In addition, the exercise works well for examining roles within an organization, the tasks SOC personnel should conduct, and what should be pointed out to other staff members.

Acknowledging these dimensions and safely testing or even challenging them during the exercise can be an advantage for an organization in situations of cyber incidents. It is known from previous studies that simulation training ought to be meaningfully designed (Nestel et al., 2018). According to the present study, the meaningfulness of organizational learning in cybersecurity exercises is strongly related to the processes and operations of organizations. Several actions, processes, and knowledge types were improved; however, there were also challenges in changing some of the organizations' processes and those that interfaced with collaborators' processes. Furthermore, the present study showed that it is important for organizations to explore and learn which processes and operations ought to follow laws and company policies, and which can be normalized or non-normalized because of company or team preferences. Moreover, for agile operations and lean thinking, an organizational

culture that allows for uncertainty and failures is needed to enable continuous learning and development (Leso et al., 2023). However, some uncertainties and failures can be faced and mitigated during the exercises. In addition, if the processes are clearer due to exercising, the organization is more mature to perform in the case of cyber incidents. The organization is also more prepared to develop its competencies and processes during a cybersecurity alert and, thus, more mature to respond to complex cyber threats.

It is relevant to ask whether the shift from exercising individual skills or the skills of one organization to exercising organizational processes, which can also interface with the processes of other organizations, is also a significant shift in the approaches to exercising. By exercising the interfacing processes, the organizations not only learn to train as they fight, as the common saying suggests, but leave them room to train while they fight because they have faced similar situations and solved similar issues with their collaborators. This shift in training culture increases the maturity of organizations and can, thus, be a significant advantage for organizations facing cyber incidents.

Another cybersecurity-related feature related to organizational knowledge creation and learning (Basten & Haamann, 2018; Nonaka & Konno, 1998). The processes and roles related to cybersecurity in organizations are complex because of intertwining systems and processes with other organizations. Despite these organizations sometimes taking part in the exercises at the same time, the actions leading to changes and learning would require socialization, externalization, combination, and internalization phases in all these organizations. However, it appears to be challenging to have the required support from management to conduct the changes inter-organizationally, let alone in several organizations at the same time. With the digital transformation enabled by rapid technological development, organizations need to be able to change their operations, ways of working, and organizational structures in an agile way.

ACKNOWLEDGMENT

The research is partially funded by the Food Chain Cyber Resilience project, European Regional Development Fund (EURA2014/12114/09 02 01 01/2021/PL). The authors wish to thank the security-related organizations that were willing to allow their workforce to participate in the interviews.

REFERENCES

Adams, J. (2015). Conducting semi-structured interviews. In J. Wholey, H. Hatry, & K. Newcomer (Eds.), *Handbook of practical program evaluation* (4th ed., pp. 492–505). Jossey-Bass. doi:10.1002/9781119171386.ch19

Amis, J. (2005) Interviewing for case study research. In D. L. Andrews, D. S. Mason, & M. L. Silk (Eds.), Qualitative methods in sports studies (pp. 104–138). Berg.

Antunes, H., & Pinheiro, P. G. (2020). Linking knowledge management, organizational learning and memory. *Journal of Innovation & Knowledge*, *5*(2), 140–149. doi:10.1016/j.jik.2019.04.002

Argyris, C. (2002). Double-loop learning, teaching, and research. *Academy of Management Learning & Education*, *1*(2), 206–218. doi:10.5465/amle.2002.8509400

Argyris, C. (2004). Double-loop learning and implementable validity. In H. Tsoukas & N. Mylonopoulos (Eds.), *Organizations as knowledge systems* (pp. 29–45). Palgrave Macmillan. doi:10.1057/9780230524545_2

Argyris, C., & Schön, D. A. (1996). *Organizational learning II: Theory, method and practice*. Addison-Wesley.

Argyris, C., & Schön, D. A. (1997). Organizational learning: A theory of action perspective. *Reis*, *77/78*(77/78), 345–348. doi:10.2307/40183951

Aydan, S., & Kaya, S. (2018). Ethical climate as a moderator between organizational trust and whistle-blowing among nurses and secretaries. *Pakistan Journal of Medical Sciences*, *34*(2), 429–434. doi:10.12669/pjms.342.14669 PMID:29805421

Bakker, A. B. (2011). An evidence-based model of work engagement. *Current Directions in Psychological Science*, *20*(4), 265–269. doi:10.1177/0963721411414534

Breu, R., Dustdar, S., Eder, J., Huemer, C., Kappel, G., Kopke, J., Langer, P., Mangler, J., Mendling, J., Neumann, G., Rinderle-Ma, S., Schulte, S., Sobernig, S., & Weber, B. (2013). Towards living inter-organizational processes. In *15th Conference on Business Informatics* (pp. 363–366). IEEE.

Brilingaitė, A., Bukauskas, L., & Juozapavičius, A. (2020). A framework for competence development and assessment in hybrid cybersecurity exercises. *Computers & Security*, *88*, 101607. doi:10.1016/j.cose.2019.101607

Capano, D. E. (2021, September 30). *Throwback attack: How NotPetya accidentally took down global shipping giant Maersk*. Industrial Cybersecurity Pulse. https://www.industrialcybersecuritypulse.com/threats-vulnerabilities/throwback-attack-how-notpetya-accidentally-took-down-global-shipping-giant-maersk/

Chapman, S., Smith, R., Maglaras, L., & Janicke, H. (2017). Can a network attack be simulated in an emulated environment for network security training? *Journal of Sensor and Actuator Networks*, *6*(3), 16. doi:10.3390/jsan6030016

Cheung, R. S., Cohen, J. P., Lo, H. Z., Elia, F., & Carrillo-Marquez, V. (2012). Effectiveness of cybersecurity competitions. In *Proceedings of the international conference on security and management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Dadzie, J., Runeson, G., Ding, G., & Bondinuba, F. K. (2018). Barriers to adoption of sustainable technologies for energy-efficient building upgrade—Semi-structured interviews. *Buildings*, *8*(4), 57. doi:10.3390/buildings8040057

Drejer, A. (2000). Organisational learning and competence development. *The Learning Organization*, *7*(4), 206–220. doi:10.1108/09696470010342306

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* (pp. 176–191). Carol I National Defence University Publishing House.

Engström, A., & Käkelä, N. (2019). Early steps in learning about organizational learning in customization settings: A communication perspective. *The Learning Organization*, *26*(1), 27–43. doi:10.1108/TLO-09-2018-0150

Ferguson, B., Tall, A., & Olsen, D. (2014). *National cyber range overview. 2014 IEEE Military Communications Conference*.

Frank, M., Leitner, M., & Pahi, T. (2017). Design considerations for cyber security testbeds: A case study on a cyber security testbed for education. In *2017 IEEE 15th International Conference on Dependable, Autonomic and Secure Computing* (pp. 38–46). doi:10.1109/DASC-PICom-DataCom-CyberSciTec.2017.23

Gill (2003).

Hatfield, J. M. (2018). Social engineering in cyber security: The evolution of a concept. *Computers & Security*, *73*, 102–113. doi:10.1016/j.cose.2017.10.008

Heide, J. B., & Miner, A. S. (1992). The shadow of the future: Effects of anticipated interaction and frequency of contact on buyer-seller cooperation. *Academy of Management Journal*, *35*(2), 265–291. doi:10.2307/256374

Henkel, M., Koutsopoulos, G., Bider, I., & Perjons, E. (2019). Using the fractal enterprise model for inter-organizational business processes. *38th International Conference on Conceptual Modeling (ER 2019)*.

Howe, S. E., & Anda, B. (2005). Experiences from conducting semi-structured interviews in empirical software engineering research. *11th IEEE International Software Metrics Symposium (METRICS 2005)*.

Karjalainen, M. (2021). *Pedagogical basis of live cybersecurity exercises*. JYU dissertations.

Karjalainen, M., & Kokkonen, T. (2020). Comprehensive cyber arena: The next generation cyber range. In *2020 IEEE European symposium on security and privacy workshops* (pp. 11–16). IEEE. doi:10.1109/EuroSPW51379.2020.00011

Karjalainen, M., Kokkonen, T., & Puuska, S. (2019). Pedagogical aspects of cyber security exercises. In *2019 IEEE European symposium on security and privacy workshops* (pp. 103–108). IEEE. doi:10.1109/EuroSPW.2019.00018

Karjalainen, M., & Ojala, A.-L. (2022). Authentic learning environment for in-service trainings of cyber security: A qualitative study. *International Journal of Continuing Engineering Education and Lifelong Learning*, *1*(1).

Killingsworth, J. M., & Jones, B. G. (1989). Division of labor of integrated teams: A crux in the management of technical communication. *Technical Communication (Washington)*, *36*(3), 210–221.

Kim, J., Kim, K., & Jang, M. (2019). Cyber-physical battlefield platform for large-scale cybersecurity exercises. In *2019 11th international conference on cyber conflict (CyCon)* (Vol. 900, pp. 1–19). IEEE. doi:10.23919/CYCON.2019.8756901

Kolb, D. A. (1984). *Experiential learning: Experience as the. source of learning and development*. Prentice Hall.

Kolb, D. A., Boyatzis, R. E., & Mainemelis, C. (2001). Experiential learning theory: Previous research and new directions. In R. J. Sternberg & L.-f. Zhang (Eds.), *Perspectives on thinking, learning, and cognitive styles* (pp. 227–247). Lawrence Erlbaum Associates Publishers.

Leitner, M., Frank, M., Langner, G., Landauer, M., Skopik, F., Smith, P., Akhras, B., Hotwagner, W., Kucek, S., Pahi, T., Reuter, L., & Warum, M. (2021). Enabling exercises, education and research with a comprehensive cyber range. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, *12*(4), 37–61.

Leso, B. H., Cortimiglia, M. N., & Ghezzi, A. (2023). The contribution of organizational culture, structure, and leadership factors in the digital transformation of SMEs: A mixed-methods approach. *Cognition Technology and Work*, *25*(1), 151–179. doi:10.1007/s10111-022-00714-2 PMID:36118918

Lindsay, A., Downs, D., & Lunn, K. (2003). Business processes – attempts to find a definition. *Information and Software Technology*, *45*(15), 1015–1019. doi:10.1016/S0950-5849(03)00129-0

Liu, H., Han, W., & Jia, Y. (2019). Construction of cyber range network security indication system based on deep learning. In *2019 IEEE 4th International Conference on Data Science in Cyberspace (DSC)*, 495–502. doi:10.1109/DSC.2019.00081

Luecke, R. (2003). *Managing change and transition*. Harvard Business School Press.

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)* (pp. 27–36). IEEE. doi:10.1109/EuroSPW51379.2020.00013

Metz, M. (2021). Overview of change in organizations. Resistance to change. A literature review. *"Ovidius" University Annals, Economic Sciences Series, 21*(1).

Moser, A., & Cohen, M. I. (2013). Hunting in the enterprise: Forensic triage and incident response. *Digital Investigation*, *10*(2), 89–98. doi:10.1016/j.diin.2013.03.003

Murray, P., & Donegan, K. (2003). Empirical linkages between firm competencies and organisational learning. *The Learning Organization*, *10*(1), 51–62. doi:10.1108/09696470310457496

Nestel, D., Krogh, K., & Kolbe, M. (2018). Exploring realism in healthcare simulations. In D. Nestel, M. Kelly, B. Jolly, & M. Watson (Eds.), Healthcare simulation education: Evidence, theory and practice (pp. 53–62). John Wiley & Sons.

Nonaka, I. (1994). A dynamic theory of organizational knowledge creation. *Organization Science*, *5*(1), 14–37. doi:10.1287/orsc.5.1.14

Nonaka, I., & Konno, N. (1998). The concept of Ba: Building a foundation for knowledge creation. *California Management Review*, *40*(3), 40–54. doi:10.2307/41165942

Nonaka, I., & Takeuchi, H. (1995). *The knowledge-creating company: How Japanese companies create the dynamics of innovation*. Oxford University Press.

O'Connor, T. J., & Stricklan, C. (2021). Teaching a hands-on mobile and wireless cybersecurity course. In *Proceedings of the 26th ACM conference on innovation and technology in computer science education* (Vol. 1, pp. 296–302). doi:10.1145/3430665.3456346

Pham, C., Tang, D., Chinen, K. I., & Beuran, R. (2016) Cyris: A cyber range instantiation system for facilitating security training. In *Proceedings of the seventh symposium on information and communication technology* (pp. 251–258). doi:10.1145/3011077.3011087

Polanyi, M. (1966). *The tacit dimension*. Routledge and Kegan Paul.

Richter, I., Raith, F., & Weber, M. (2016). Problems in agile global software engineering projects especially within traditionally organised corporations: An exploratory semi-structured interview study. In *Proceedings of the 9th International C* Conference on Computer Science & Software Engineering* (pp. 33–43). doi:10.1145/2948992.2949019

Robinson, V. M. J. (2001). Descriptive and normative research on organizational learning: Locating the contribution of Argyris and Schön. *International Journal of Educational Management*, *15*(2), 58–67. doi:10.1108/EUM0000000005395

Robinson, V. M. J. (2002). Organizational learning, organizational problem solving and models of mind. In K. Leithwood, P. Hallinger, G. C. Furman, K. Riley, J. MacBeath, P. Gronn, & B. Mulford (Eds.), Second international handbook of educational leadership and administration (pp. 777–812). Springer. doi:10.1007/978-94-010-0375-9_26

Robinson, V. M. J. (2014). Single- and double-loop learning. In D. C. Phillips (Ed.), *Encyclopedia of educational theory and philosophy* (pp. 754–756). Sage.

Rosemann, M., & de Bruin, T. (2005). Towards a business process management maturity model. In D. Bartmann, F. Rajola, J. Kallinikos, D. Avison, R. Winter, & P. Ein-Dor (Eds.), *13th European Conference on Information Systems*. Academic Press.

Sarıkaya, Ş., & Kara, B. K. (2020). Organizational trust and organizational support as a predictor of job satisfaction. *International Journal of Curriculum and Instruction*, *12*, 435–466.

Schulz (2017).

Schweiger, S., Stouten, H., & Bleijenbergh, I. L. (2018). A system dynamics model of resistance to organizational change: The role of participatory strategies. *Systems Research and Behavioral Science*, *35*(6), 658–674. doi:10.1002/sres.2509

Scott, W. R. (2013). Institutions and organizations. Ideas, interests, and identities. *Sage (Atlanta, Ga.)*.

Sinha, K. (2014). *Structural complexity and its implications for design of cyber-physical systems* [doctoral dissertation]. Massachusetts Institute of Technology.

Skirpan, M. (2018). Quantified self: An interdisciplinary immersive theater project supporting a collaborative learning environment for CS ethics. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education* (pp. 946–951). Association for Computing Machinery. doi:10.1145/3159450.3159574

Švábenský, V. (2020). What are cybersecurity education papers about? A systematic literature review of SIGCSE and ITiCSE conferences. In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education* (pp. 2–8). Association for Computing Machinery. doi:10.1145/3328778.3366816

Törngren, M., & Grogan, P. T. (2018). How to deal with the complexity of future cyber-physical systems? *Designs*, *2*(4), 40. doi:10.3390/designs2040040

Utterback, J. M. (1971). The process of technological innovation within the firm. *Academy of Management Journal*, *14*(1), 75–88. doi:10.2307/254712

Von Solms, R., & van Niekerk, J. (2013). From information security to cybersecurity. *Computers & Security*, *38*, 97–102. doi:10.1016/j.cose.2013.04.004

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). *Lessons learned from complex hands-on defence exercises in a cyber range. In 2017 IEEE frontiers in education conference*. FIE.

Walton, H. (2022, September 11). *The Maersk cyber attack – How malware can hit companies of all sizes*. Kordia. https://www.kordia.co.nz/news-and-views/the-maersk-cyber-attack

Warner, M. (2012). Cybersecurity: A pre-history. *Intelligence and National Security*, *27*(5), 781–799. doi:10.1080/02684527.2012.708530

Wilson, E. J., & Nielson, C. C. (2001). Cooperation and continuity in strategic business relationships. *Journal of Business-To-Business Marketing*, *8*(1), 1–24. doi:10.1300/J033v08n01_01

Yamin, M. M., & Katt, B. (2022). Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, *116*, 102635. doi:10.1016/j.cose.2022.102635

Zhao, X., Zhao, S., Liu, N., & Liu, P. (2021). Willingness to report medical incidents in healthcare: A psychological model based on organizational trust and benefit/risk perceptions. *The Journal of Behavioral Health Services & Research*, *48*(4), 583–596. doi:10.1007/s11414-021-09753-5 PMID:33851309

Mika Karjalainen holds a PhD in information technology. He works currently in the Jamk University of Applied Sciences as a director of the School of Technology and conducting research in the field of cyber security education.

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.