jamk

# Pre-assessing Cyber Range-Based Event Participants' Needs and Objectives

## Literature Review

Jani Päijänen

Master's thesis
December 2023
School of Technology
Master's Degree Programme in Information Technology
Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

**Description**

**Päijänen, Jani**

**Pre-assessing Cyber Range-Based Event Participants' Needs and Objectives**

Jyväskylä: Jamk University of Applied Sciences, December 2023, 60 pages

Degree Programme in Cyber Security. Master's thesis.

Permission for open access publication: Yes

Language of publication: English

**Abstract**

Cyber arena and cyber range-based cyber exercises and trainings are widely considered beneficial for learners; technical cyber security is best learnt hands-on. In addition to technical Information and Communication technology (ICT) and cyber security experts, organisations' other roles can benefit participating to an exercise. The technical platforms have been applied to bridge the skills gap in cybersecurity, both full-time technical ICT and cyber security professionals, and those needed cyber security knowledge, skills and understanding in their daily work.

To understand what cyber range-based exercise and cyber lab-based capture the flag (CTF) participants prefer, a pre-exercise survey was conducted. It was also evaluated, if the used survey can be utilized to acquire areas of interest from the participants and know their backgrounds better, to plan and develop exercise content and answer to participants' needs. The survey and the research were documented in the article "Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones" by Päijänen et al. (2023).

The survey results indicate that participants prefer technical contents over non-technical, although non-technical contents were reported too. Due the setup of the survey, potential bias was recognised and therefore more research is needed. The evaluation indicated that the survey itself can be used to get needs and wishes from exercise participants, which in turn can help exercise planner to provide highly valuable cyber range-based exercises.

Information gathering from databases was performed to reach the research objectives. However, the data about participant's needs prior an exercise, turned out be thin, at least per used databases and search terms. More research is needed to understand state of the art in end-user, or customer, understanding what comes to cyber security exercises. Porter's (1991) theories of value chain and value system was supposed to be used to map participants and their needs of exercise contents. Due the low number of included research articles, maturity of the mapping could not have been higher.

**Keywords/tags (subjects)**

Cyber security, cyber range-based exercises, participant & customer understanding

**Miscellaneous**

Number of pages in References (9) and Appendices (13) is 22. No confidential information in this thesis.

**Contents**



**Figures**

**Tables**

**Terms and Abbreviations**

| | |
|---|---|
| **APT** | Advanced Persistent Threat |
| **Blue Team** | The target audience of CA-based exercises and CRXs. |
| **Company** | See Organisation |
| **CA** | Cyber Arena |
| **CL** | Cyber Lab |
| **CLX** | Cyber Lab-based Exercise |
| **CR** | Cyber Range |
| **CROF** | Cyber Range Operational Federation. CRs share e.g., exercise contents, with each other. |
| **CRTF** | Cyber Range Technical Federation. A CR utilises federated CRs capabilities, features and functionalities to offer more feature rich CSE and evading investment costs. |
| **CRX** | Cyber Range-based Exercise |
| **CS** | Cyber Security |
| **CSC** | Cyber Security Competition |
| **CSE** | Cyber Security Exercise (can be either a tabletop or CRX) |

| | |
|---|---|
| **CST** | Cyber Security Training |
| **CSX** | Cyber Security Exercise. Can be any of e.g., tabletop, CRX, CLX or some combination. |
| **CTF** | Capture the Flag. Can be either defensive or offensive |
| **DFIR** | Digital Forensics and Incident Response |
| **EQF** | European Qualifications Framework for Lifelong Learning |
| **ICT** | Information and Communication Technology |
| **KSA** | Knowledge, Skills, Abilities |
| **Organisation** | The term *organisation* refers to both companies and organisations if not otherwise expressed |
| **Red Team** | Red Team (RT) that simulates threat actors' Tactics, Techniques and Procedures (TTP) in CRXs or CA-based CSEs. |
| **RGCE** | Realistic Global Cyber Environment, a Cyber Arena (CA) |
| **RQ** | Research Question |
| **SCADA** | Supervisory Control And Data Acquisition. |
| **TTP** | Tactics, Techniques and Procedures. (Cyber) Threat actors usually have their own signature made by these. |

# 1 Introduction

## 1.1 Background of the Research

The number of available cyber security professionals with appropriate skills has been a recognised issue now for a few years. It is estimated that globally employers demand for from two to over three million cyber security experts. World Economic Forum, based on the data provided by ISC2, an association of cyber security professionals, estimated 3.4 million cyber security experts' shortage globally (World Economic Forum, 2022). In the EU it is estimated that some 300 000 persons are needed to fulfil the demand (European Union Agency for Cybersecurity (Enisa), 2023). US based CyberSeek's (2023) service shows that employers in the US can fill 72% of cybersecurity job demand, and that between September 2022 and August 2023 there were total 572,392 job openings in cybersecurity, resulting roughly 160,000 open and not filled positions. In the UK a shortfall of c. 11,200 individuals was estimated (Coutinho, et al., 2023). The situation of Finland was reported (Lehto, 2022) in terms of full-time cyber security professionals demand and existing employees that require cyber security in their work, and which need to develop of new skills in cyber security. Fulltime demand in Finland was estimated between 5,000 – 8,000 persons and upskilling or retraining between 6,000 – 13,000 persons. Lehto's report lists estimations based on NICE frameworks' work role listing (Newhouse, Keith, Scribner, & Witte, 2017).

There is a global demand for cybersecurity professionals having knowledge, skills and competencies required for the task. Supplying full-time cyber security professionals and other roles that require cyber security knowledge, skills and abilities in their daily work can be done either by the education system, or training existing cyber security, ICT, and other professionals, by retraining or upskilling. Lagner et al. (2022) stated that the cyber security threats in the digital environment, challenge organisations and persons, as it is no longer enough individuals to demonstrate solely knowledge, but skills and abilities are needed too. Also, they state that cyber security (CS) future education courses must utilise cyber ranges to learn hands-on cyber security instead of being just (mass) lecture and theoretical in contents. Similar statements, that learning environments should be authentic, was said by e.g., by Karjalainen in his dissertation thesis (Pedagogical Basis of Live Cybersecurity Exercises, 2021). Švábenský et al. (2022) state that [university (authors note)] students in cyber security need to develop practical skills, and that most straightforward to do that are hands-on exercises. Lehto (2022) propose measures not only education system, but training of

professional, elders and children too. He mentions that also non-technical training should be offered in Finland. Large companies and organisations situation was reported to be good. SMEs, although low priced training were available, reportedly did not acquire it, partly because of SMEs do not recognise what cyber security training should be taken, nor the training organisations know that trainings would be interested in the market (Lehto, 2022).

Each of Lagner et al. (2022), Karjalainen (2021) and Švábenský et al. (2022), propose cyber ranges (CRs) or cyber arenas (CAs) as an environment to train, learn and study cyber security hands on handles. In addition, the learners can be exposed to technical cyber security also in smaller scale environments, i.e., cyber-labs (CLs). CRs, CAs, and CLs are safe and controlled technical environments which can be used e.g., in cyber security exercises (CSE), competitions (CSC), trainings (CST), and curriculum courses. Not only can CAs, CRs and CLs be used for technical contents, but also procedural and operational security controls related contents could also be included.

Cyber security Body of Knowledge (CyBOK) version 1.1 listed five knowledge areas of cyber security, each having more detailed concepts underneath. The concepts, or knowledge areas (KAs) were Human, Organisational and Regulatory Aspects; Attacks and Defence; Systems Security; Software and Platform Security; and Infrastructure Security (CyBOK, 2021). These CyBOK's concepts could be exercised, trained, or competed in. To an extent, it is advisable too. So, in addition to technical cyber security contents, the resulting learning event could have contents, including but not limited to, top-management, public relations and communications, and the technical ICT and cybersecurity specialists (Päijänen, et al., 2022).

Based on our experience, in CRXs the exercise's objectives relate to learning. The learning objectives are either visible and explicitly expressed or hidden and implicit objectives. The learning objectives may have been exposed to the target audience or may not. CRX objectives may include a bullet point indicating that a specific technology will be tested in conjunction with the exercise. Then the technology's fulfilment of requirements, or its applicability to some scenario or environment is tested. The persons involved with the technology, and broader, persons participated into a CRX, can learn *something,* regardless of are the learning outcomes aligned with the set objectives or not.

In the EU funded project, CyberSec4Europe (European Union (EU), 2023), two cross-border, online-only two-day Flagship CSXs were conducted. Flagship 1 exercise was conducted in January 2021 (Päijänen, Viinikanoja, & Piispanen, 2021) and Flagship 2 in January 2022 (Päijänen, Piispanen, & Viinikanoja, 2022). Besides the exercise learning contents, both exercises acted as technology demonstrators (Kokkonen, Sipola, Päijänen, & Piispanen, 2023). After the Flagship 1 CRX, a pre-survey for the forthcoming Flagship 2 CSX was drafted. It was planned to be tested with Flagship 2 CSX enrollers before the exercise (Karinsalo, Saharinen, Päijänen, & Salonen, 2022). The plan was successful.

This study is based on the article "Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones" (Päijänen, Salonen, Karinsalo, Sipola, & Kokkonen, 2023). The preliminary survey results were described and analysed in that research article.

## 1.2 Research Article

The research article authored by Päijänen et al. (2023) focused on researching the applicability of the cyber security exercise pre-survey drafted by Karinsalo et al. (2022) and analyses the executed survey results. Would the pre-survey be applicable, then cyber exercise planners could utilize the survey and by analysing its results, plan exercises more effectively meeting the needs and interests of the exercise participants. The article was proposed and accepted to ECCWS 2023. It was published in Proceedings of the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023 by Academic Conferences International Limited.

The research article was written after the pre-survey of Flagship 2 event, and after the CRX and CLE itself was executed. The Flagship 2 event contained two parallel activities:

1. A defensive cyber range-based exercise (CRX)
2. A defensive, open, CL-based exercise (CLE), a capture the flag (CTF)

The participants' task was to perform digital forensics and investigation to an already happened fictional cyber security incident. The incident was prepared in Realistic Global Cyber Environment

(RGCE), a CA that was owned and operated by Jamk University of Applied Science's Institute of Information Technology's cyber security research, development and training center, JYVSECTEC (JYVSECTEC, 2022). The digital evidence of the incident was exported and offered to the participants of the activity #2, forming in total CTF six challenges. The event applicants were able to register to single activity only. Equal pre-surveys were offered to the enrollers of both activities.

The questions from one to six were background questions. The first question of the pre-survey was E-mail address (Table 1). Educational background was asked in question #2, to know the respondents better. It was a multiple-choice question, and the categorisation was done according to the European Qualifications Framework (EQF) (Council of the European Union, 2017). Additionally, there was a "Other, please specify" in case the respondent didn't belong or did not recognise any of the options. Background question #3, the primary sector of respondent's organisation was a single-choice question. The categorisation followed the sectors specified in the European Cybersecurity Taxonomy (2019). Respondents were backed up with an additional option "Other, please specify". The fourth single-choice background question followed Bloom's taxonomy (Bloom, 1956). Respondents' self-estimation of their competence level in CSX in general was enquired. The same Bloom taxonomy was used in background question #5, where respondents were asked to self-evaluate their technical skills regarding CSX or hackathons. The sixth background question was a single-choice, following sectors specified in the NIST – National Initiative for Cyber security Education (NICE) Cybersecurity Workforce Framework (Newhouse, Keith, Scribner, & Witte, 2017). The options were supported by option" Other, please specify". The Sixth question enquired respondent's primary job role.

The options of question #7 were applied from (Karinsalo & Halunen, Design of Education and Professional Framework, 2021), and it enquired respondents most interesting development or improvement knowledge areas. Respondents had to choose between one to three options. In question eight, preferred knowledge area to progress during the exercise, i.e., preferred exercise role was enquired, and it the categorisation was applying according to Newhouse et al. (2017). In question nine, the ideal number of participants in exercise teams were asked to be selected from a single-choice list. The exercise session duration was enquired in question #10. In question #11 the least interesting development or improvement knowledge areas were enquired, applied from Karinsalo and Halunen (2021). Question #12 was an open question.

Table 1: Pre-survey background and research questions

| Background questions | Research questions |
|---|---|
| 1. E-mail address | 7. Most interesting development or improvement knowledge areas |
| 2. Educational background | 8. Preferred knowledge area to progress during the exercise |
| 3. Primary sector of the respondent's organisation | 9. Ideal number of participants in exercise's teams |
| 4. Knowledge related to cyber security exercise or hackathons | 10. Average exercise session duration (i.e. how often does the exercise/situation develop) |
| 5. Technical skills related to cyber security exercise or hackathons | 11. Least interesting development or improvement knowledge area |
| 6. Primary job role | 12. Free text feedback, comments, concerns |

We wanted to understand if the Karinsalo's et al. (2022) pre-survey could provide insights to understand CRX enrollers' backgrounds, their self-assessed expertise, interest areas, and their needs regarding to Flagship 2 CRX and CLX. This information could potentially be then used to modify the contents of the respective activity, or to provide contents in the future CRXs or CLX, responding to the reported need. Three main research questions (RQs) were selected for guidance. They were:

> **RQ1 How can we improve the quality of a cyber-exercise through pre-assessment of the participants?**
>
> **RQ1.1 How can we enhance the participant experience within a specific cyber-exercise?**
>
> **RQ2 What are the most and least interesting topics in a cyber-exercise?**
>
> (Päijänen, Salonen, Karinsalo, Sipola, & Kokkonen, 2023)

The preliminary survey was targeted at the registered participants, instead of a broader audience.

In the activity #1, defensive CRX participants were placed into *blue teams*, and each team had members from several organisations. Each team was supported by a dedicated team coach, who led the team with questions and assisted participants with the available tools. The CSX participants learnt new skills and abilities (Kokkonen, Päijänen, & Sipola, 2023; Päijänen, Piispanen, & Viinikanoja, 2022).

In the activity #2, open defensive CTF, participants worked independently, i.e., no teams were formed. An after-action survey was out of scope for the CTF. However, we came into conclusion, based on *in-situ* chat messages, submissions statistics of the CTF event, and the time participants spent with the CTF challenges, that there was demand for such event (Päijänen, Piispanen, & Viinikanoja, 2022).

### 1.2.1 Data Analysis

Data analysis was done utilising Microsoft Excel. The analysis steps were:

Step 1: Data merge
Step 2: Data cleansing
Step 3: Data anonymisation
Step 4: Initial analysis
Step 5: Data insertion
Step 6: Data analysis
Step 7: Conclusions

In Step #1, data from two surveys, surveys for registered of activity #1 and #2, was merged into a single excel table. A column was added to indicate the activity respondent requested, i.e., CRX or CTF. In the next step the data quality was checked, whether data cleansing was needed, i.e., removing possible duplicate entries, or removing test entries by authors and testers. In step #3 the data rows were anonymised, i.e., respondent's email addresses were replaced with coded strings. Initial analysis in step #4 revealed the need to have more uniting, or summarising, values in respondent's organisation primary sector. Therefore, in step #5, a new column was inserted to the dataset. The column was populated with one of the options "Industry", "Public Sector", and "I prefer not to disclose this information", based on the initial answers to the research question #3. In

step #6 the data was analysed across several excel sheets and tables therein. Finally, the conclusions were made and reported on the article.

### 1.2.2 Ethically and Reliability of the Research Article

In the marketing outreach potential participants were informed what can be expected from the two-days, which was technical contents, but no detailed information was provided.

The research survey was conducted prior the actual event. The respondents of activity #1, defensive CRX, were expected to have legal capacity as they were expected be in an employment relationship with an affiliated CyberSec4Europe partner. This was verified by manually screening the reported email addresses domain part; it had to match with the known domain address of the affiliate. Also, certain logic was implemented to the registration form to prevent non-affiliates registering to the CRX.

The respondents of the activity #2, defensive, open, CTF exercise, a CLX, were asked in the registration form if they were 18-years of age already. Negative answer would not have let the registration flow through.

In the registration form respondents of both activities were asked permission to use their non-identifiable reported answers in research, and additionally they were asked permission to be contacted after the exercise, either to be interviewed or asking to participate in a research survey.

Flagship 2's open CTF activity was marketed in three social media services: then-Twitter, Instagram, and LinkedIn. Organic presence was carried out by a webpage of Jamk University of Applied Sciences, a webpage of CyberSec4Europe project. A press-release by Jamk was published and it was noticed by three major Finnish ICT-media services and two Finnish financial and investment media, having several hundred thousand weekly readers combined. The exercise activity of Flagship 2 was marketed to CyberSec4Europe project affiliates via email, through the web pages and social media posts (Päijänen, Piispanen, & Viinikanoja, Flagship 2, 2022).

The order of activities and the participants or targets of those activities is important when thinking of reliability of the research, specifically the following:

- the marketing actions of the event were executed before the preliminary survey was conducted, and
- marketing message was “welcome to attend to a technical defensive CRX or a defensive CTF”, and
- the preliminary survey response requests were sent only to event registrants.

We assume that the survey respondents were exposed to the marketing message and thus knew where they were about to participate and what learning contents, at least at the topic level, they would soon have access to. We expect the marketing message reached (mostly) technically oriented persons. This may have caused bias. New runs with the pre-survey could be done, with different order of actions, so that respondents with non-technical backgrounds could be acquired. The order of the pre-survey’s options was static. Would the order have been randomised; perhaps different results would have been acquired.

### 1.2.3 Conclusions of the Research Article

Data analysis of the research article revealed that no remarkable differences between CSX and CTF respondents existed. Participants of both activities preferred technical CSX or CTF contents instead of other options. Viewed from participants backgrounds, the same applies, i.e., technical contents were reported to be interesting. Least interesting exercise contents were societal security, human security, and organisational security. Societal security covers cybercrime, law, policy, and privacy topics, whereas Human security includes, e.g., identity management, social engineering, awareness and understanding, and usable security and privacy (Päijänen, Salonen, Karinsalo, Sipola, & Kokkonen, 2023). The direction of legislation and regulations *seem* to deal with at least the procedural and technical parts of cyber security. The authors are yet unaware if there are legislative or regulatory requirements about operational security. Human security is currently highly effective attack vector. Various phising emails and CEO frauds are being used. Even defensive technology develops, such emails and a like will get through. Therefore top-management, employees, students, etc. should be aware of those and have the understanding how to deal with them. When the human security controls are exploited, there might be change that technical controls are exploited too. Then the next line of defence are the organisational controls. In case of organisational controls are applied, then incident management and business continuity plans are executed.

Those topics can and should be covered other kind of CSXs and trainings. The elsewhere collected data shows that CSXs develop participants KSAs.

### 1.3 Author's Contribution

The author was responsible for the data-analysis and data-analysis contents in the article and participated in planning and writing the article. In addition, the author drafted presentation materials and presented the article in the 22nd European Conference on Cyber Warfare and Security, ECCWS 2023.

### 1.4 Structure of the Thesis

In the previous chapters presented i) overview of the research subject, ii) introduction to the conducted research, iii) the research, iv) self-assessed research's ethicality and reliability of the research, and v) author's contribution. Research question and methodology is discussed in chapter 2. Theoretical framework is presented in chapter 3. Literature review is presented in chapter 4. Conclusions and further ideas are presented in chapter 5.

## 2 Research Question and Methodology

To guide and focus authors' work, after several iterations two questions were raised. One research question, and one support question. The research question, after several iterations, evolved into:

> How are participants' learning needs, objectives or priorities considered in planning cyber range-based exercises?

The support question was:

> How does literature indicate that Porter's value chain (Porter, 1991) has been applied when participating organisations selected participants to a cyber range-based exercise?

The research question tries to understand whether exercises are mostly setup from the exercise's conductor point of view, or up to what level are participants needs, wishes or objectives considered. If such needs were gathered prior an exercise, it indicates that customisation of exercise contents could be done. The more customisation is done, the longer the exercise lifecycle states' duration preceding the actual exercise execution would be. Vykopal et al. (2017)lists four cyber range-based exercise lifecycle states as 1) Preparation, 2) Dry run, 3) Execution, and 4) Evaluation. Highly productised CRXs lifecycle states prior the exercise will take *about* constant time after the initial investment, i.e., after the exercise has been once conducted. The *assumption* is that organisers of mass executed cyber range-based exercises are not that interested on customer's needs and expectations prior the exercise, but their interest is in the after-exercise performed user feedback and quality control.

With the support question, and its potential answers, we wanted to make cyber security more understandable within business in general, and *vice versa,* make fundamental business strategy concept known for cyber security professionals. Porter's value chain is explained in chapter 3 Theoretical Framework and Concepts. In the next chapter theories and methodologies of literature review are addressed.

## 2.1 Methodology and Theories About Literature Review

Booth et al. (2020) noted that the search process is commonly iterative, instead of linear, and responds to emergent data. They state that multiple search strategies and approaches are involved when performing literature review. Palmatier et al. (2018) emphasise that a literature review must be useful to scholars and practitioners. Renner et al. (2022) and Snyder (2019) note that writing literature reviews is becoming more complex due to the increasing amount of research papers. To assist researchers with literature reviews, software has evolved into *mature enough*, and currently more technically savvy targeted scripts and libraries exists (Ivančić, Glavan, & Vukšić, 2020; Centre for Science and Technology Studies, Leiden University, 2023; van Eck & Waltman, 2015; Pimentel, 2022; Musunuru, 2021).

The Initial idea about the methodology was to carry out a narrative literature review. Had we done that, we could have gathered the data as per our liking, perhaps pearl growing found articles, i.e., we could have directed data search process based on the found data, and potentially expanded

the data set from the initial literature research objective (Vilkka, 2023). If no strict inclusion or exclusion criteria for the data were set, as narrative literature reviews are welcomed to do, then narrative literature could echo authors' values, beliefs, and preconceptions (Vilkka, 2023; Greenhalgh, Thorne, & Malterud, 2018). Well formulated research question, and clear inclusion and exclusion criteria for the data are "a cornerstone" of systematic literature reviews. Hence the systemic approach, the data gathering process is repeatable, i.e., a researcher elsewhere can reproduce and validate the used data set, thanks to the transparency (Vilkka, 2023; Greenhalgh, Thorne, & Malterud, 2018). While narrative review is not expected similar systematic approach, they are not "ad-hoc" or careless (Greenhalgh, Thorne, & Malterud, 2018). Applying the steps of Search, Appraisal, Synthesis and Analysis (SALSA) in performing literature view - perhaps in an iterative way - was recommened by e.g. Vilkka (2023).

Combining the elements of systematic and narrative literature reviews have been suggested by many, e.g., by Collins & Fauser(2005) and Turnbull, Chugh, & Luck (2023). This is what we did. The data gathering process is transparent, used search parameters and queries are provided, as are inclusion and exclusion criteria. Then from the included articles, an analysis was done.

## 2.2 Previous Research on the Subject

Using eyeballing technique to the almost two hundred papers published between 2000-2020 and accessible from IEEE Xplore, Elsevier's ScienceDirect and Google Scholar, were found, that covered cyber range and learning or cyber range and training. Majority of the results related to machine **learning**, **training** artificial intelligence, and papers which title heavily referenced to applying or developing technology. They are not included in previous research. The few papers, which the authors had access to are presented next.

In "Crowdsourcing Approach for Developing Hands-On Experiments in Cybersecurity Education" the authors reported that about 100 papers covering hands-on cyber range learning [in university education, authors' note] was published between 2010-2019, and made the following three remarks:

1. *They show the importance of the hands-on experiments in cybersecurity education and provide some detailed methods;*

2. *They introduce solutions and technologies to develop the cyber range or the hands-on experiments;*
3. *They verify the effectiveness of the cyber ranges or the hands-on experiments.*

(Wang, Tian, & Gu, 2019)

Wolfended (Wolfenden, 2019) notes that cyber ranges are widely used by governments and industries, and that they are used to perform "hands on handles" activities. He emphasises that realistic learning environment and active learning by doing is more effective than lecture based. He mentions the skills gap, and proposes gamification as a solution, requiring gamified learning environments [i.e., cyber ranges and alike, authors note]. Lee lists five strategies regarding agencies and enterprises cyber security readiness: 1) Collaborate with the C-suite, 2) Assess cyber teams, 3) Persistently develop a cyber defence team, 4) Apply cyber skills in live fire and table-top exercises, 5) Embrace apprenticeships (Lee, 2019).

# 3 Theoretical Framework and Concepts

Cyber security is a target or end state of a system, where cyber environment can be trusted, and its functionality is secured (The Security Committee, 2018). The cyber environment covers data and information storage, edit and transfer in communication networks, and it includes the physical structures which relate to the before mentioned activities (The Security Committee, 2018).

In 1985 Porter (1991) presented the concept of value chain, which constitutes from primary and support activities, and which results to company's operating margin. By chaining and stacking multiple companies value chains, Porter presented a value system of a firm (Figure 1). Value chain and value system are one of the foundations of businesses strategy. Those concepts are known in business and in particular business strategy education, and further, in businesses' boards. Those representatives *must* understand that cyber security is necessity in company's primary and support activities, and that cyber security can be exercised and trained in those activities and at the company level. As decision makers, they are kept trusted by share- and stakeholders, ensuring business continuity. *C*yber security professionals and students *must* understand the basic concept of company's strategy. Understanding one another, business and cyber security professionals together can

eventually focus on threats and risks that *really are something* for the organisation and implement necessary risk and threat controls.

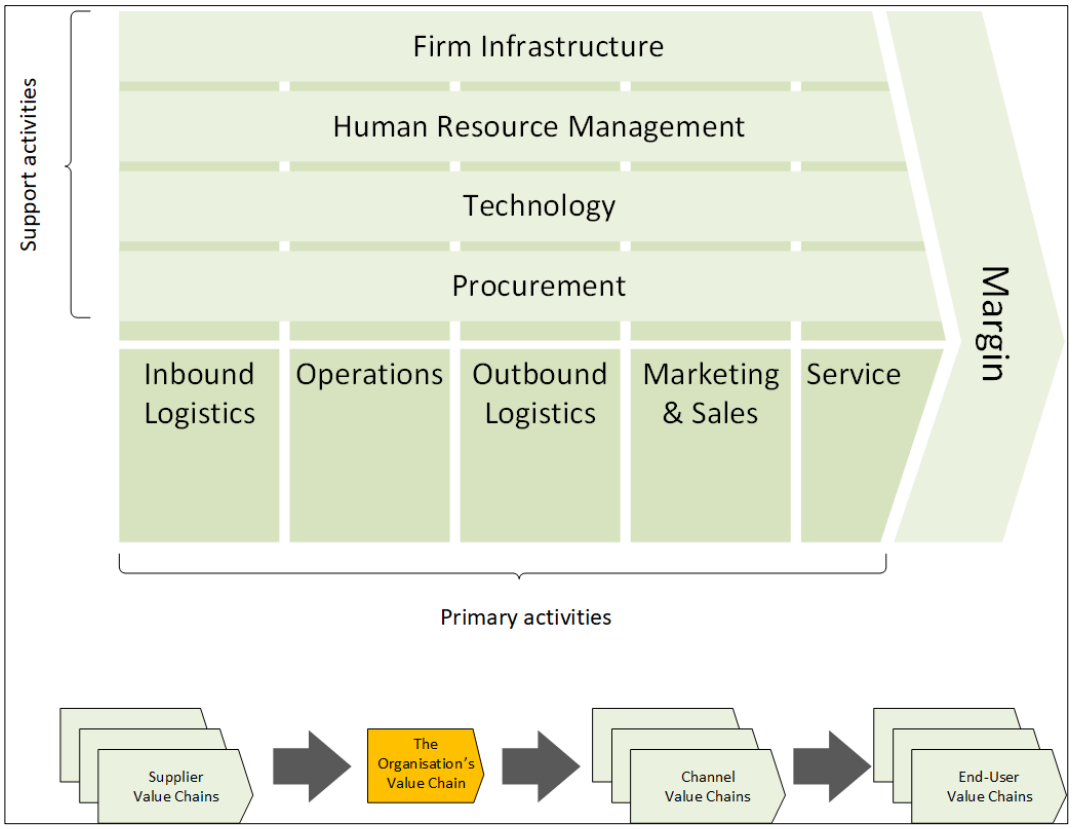


Figure 1: Value chain and value system of a company. Adopted from (Porter, 1991)

After the first appear of Porter's value chain and value system, businesses and organisations have transformed to digital, and today they are deeply interconnected via Internet. The digital and interconnectivity is not only a business mandatory, but also it brings risks. When a cyber-incident *severe enough* impacts the company's or organisation's single activity, it may have devastating cascading effect not only in its internal value chain, but in its value system. Could a cyber-attack or a cyber worm spread, then, due to the deeply interconnected value system, multiple organisations and their upstream suppliers and downstream channel partners and end-users (i.e., the value system) could be impacted. NotPetya, a state-sponsored malware, spread in 2017 in such a way. It was estimated that it caused several billions of dollars damages (Greenberg, 2018).

A cyber-attack may cause direct or indirect consequences, monetary, immaterial, intangible, tangible, or even health related consequences in the physical world. The impact of the attack may be

limited to the sole company, but it may have impact to upstream, i.e., suppliers, and downstream, i.e., channel and end-user value streams. The impact of exploited vulnerability or weakness of a control, despite of the control's nature, could be experienced in a CRX. As late as 2015, the European Union Agency for Cyber Security (ENISA) published a report, which noticed that various cyber security frameworks and standards had different perspectives to e.g., some of the then-listed frameworks recognised that only malicious activity and realised threats could only cause impact to virtual (digital) environment only, but not in physical environment. Nor would unintentional activity cause harm of any kind (Brookson, et al., 2015). If only one source was used to build organisations security controls, there are some possibilities that established controls miss certain threats or risks.

Continuing with examples of cases where risk or threat controls in a specific (Porter's) activity did unfortunately fail, next is Denmark based A.P. Møller-Maersk. It is a global maritime logistics and port operator with estimated 20% share of global maritime logistics, which was one of the victims of NotPetya. The company faced damages due lost profits, and due costs establishing the company's entire network. Greenberg (2018) mentioned that Maersk's estimated damages were some 300,000,000 USD. Just two years after the ENISA published its findings, the NotPetya malware was overflowing to the physical world from the digital world. It is possible that an incident in the digital interconnected business networks become highly visible in the physical world and is emotionally evocative.

There are other cases where a cyber-attack has had impact to thousands if not tens of thousands of organisations and companies, e.g., SolarWinds Plc (Disis & Mahmood, 2021; CyberSecurity & Infrastructure Security Agency (CISA), 2021). The company, SolarWinds, was sued by the SEC, due failing to publicly disclose the cybersecurity failures making the SolarWinds Plc hack in possible (Starks, 2023). Existing legislation can be tried to protect the interests of the government, and to defend equality of investors.

Cases from healthcare are e.g., Ireland's Department of Health and Health Service Executive (HSE, 2021), and case United Kingdom's National Health Services (National Audit Office, 2017), and case Vastaamo. Vastaamo Oy (Ltd.) was a privately held company that offered psychotherapy services in Finland. In Vastaamo case, over 30.000 patients' records, containing sensitive patient data, were

stolen in a data breach that came public in October 2020 (Finnish Broadcasting Company, 2023). Initially, Vastaamo was attempted extortion, but as no ransom were paid, it was followed by extorsion attempt of the victim patients. The then-CEO and other shareholders had sold majority of company's shares to an investment company in 2019. According to Finnish Broadcasting Company (2021), the data breach had happened a few months before the shares were sold. The Office of the Data Protection Ombudsman (ODPO) (2021) became aware of the data breach in September 2020. The ODPO stated that Vastaamo became aware of the breach already in March 2019. An administrative fine was imposed on Vastaamo in 2021 by ODPO, due non-compliance with EU's General Data Protection Regulation (The Office of the Data Protection Ombudsman, 2021).

Finland's National Bureau of Investigation received over 23.000 criminal reports and investigated the case between autumn 2020 and August 2023 (National Bureau of Investigation, 2023). The investigation revealed that there had been several data and security breaches over a period of several years (Finnish Broadcasting Company, 2023). The charges against the suspected criminal are expected to be raised during October 2023 (Finnish Broadcasting Company, 2023). The buyer's CEO stated had the data breach been disclosed, no transaction would have been done. The buyer stated a complaint about deal and sought to have roughly ten million euros in cash and other property to be confiscated. According to a Finnish commercial broadcast company, MTV Oy (2022), arbitration court ruled that the buyer will be compensated for around eight million euros, and the then-CEO had been ruled to return in full the value he received from selling the shares. In 2023, the then-CEO was found guilty "of a data protection crime because he did not fulfil General Data Protection Regulation (GDPR) requirements, in terms of the pseudonymisation and encryption of patient data handled by the center" (Finnish Broadcasting Company, 2023a), The National Supervisory Authority for Welfare and Health (Valvira) started supervision of Vastaamo on October 12, 2021, and stated that the company had neglected several of its responsibilities (Valvira, 2021). The psychotherapy company Vastaamo Oy was bankrupt in March 2021. Before the bankrupt, Vastaamo had sold its business operations, excluding IT-systems and patient records to a Finnish healthcare company (Valvira, 2021). The patients, victims of case Vastaamo, were guided by several national agencies, authorities, non-profits and cyber-volunteers (The Office of the Data Protection Ombudsman, 2020) (Kuluttajaliitto, 2020). It has been speculated that the various justice processes take several years. There were other judgements to the then-responsible of Vastaamo, too.

It is unknown to the authors, had the mentioned case organisations participated into table-top (process) exercises or CRX based exercises or not. The cases, and in particularly the exploited weaknesses or vulnerabilities could have been exercised (hindsight, yes). Attending into cyber security exercise is highly recommended, and hands-on cyber range-based exercises are best. In Hands-on technical exercises participants are exposed to the technical aspects of cyber, but there are other aspects too, but they may not be as evident but at least equally as important. These aspects are presented in the next chapter, as part of cyber security controls.

## 3.1 Cyber Security Controls

In general, cyber security controls can be split in three: procedural, operational, and technical cyber security. As the name suggests, procedural cyber security contains procedural (administrative, or management) controls, and they usually are written documents that an organisation uses for (cyber) security. Those documents include policies and procedures, e.g., various security plans, education, training, and awareness raising plans and implementation guidelines. Procedural controls are recommended to be approved and governed by the top-management. Not only are they recommended because they indicate to the organisation the direction where the management wishes to direct the organisation, but also because those documents have potential cost impact to the organisation. The impact realises when the plans and guidelines are implemented, tested, trained, and exercised. When effective, the implemented documents set expectations for employees and top management behaviour and define parties' responsibilities. Additional examples of organisations procedural controls are cyber security policy, risk management plan, or business continuity plan, and cyber-incident response plan.

Operational security, or operations security (OPSEC), is about protecting organisation's information and technology assets confidentiality, integrity, and availability (or access) and from the unlicenced (Cebula, Popeck, & Young, 2014). An example of implementing private life OPSEC is to publish a photo from a holiday trip only after the holiday, give a photo must be published in the first place. Organisational OPSEC would be e.g., not to disclose when the organisation is going to attend a cyber security exercise, against what kind of threat actors have been exercised, or who were exercising. Technical cyber security contains technical controls, i.e., countermeasures or

safeguards, which are implemented and executed by the information system, through a combination of software, firmware, and hardware (National Institute of Standards and Technology (NIST)). Examples of technical controls are Firewalls and Endpoint Detection and Response software (EDR).

## 3.2 Cyber Security Legislation and Regulation

Empirically looking at the legislation and regulation, it *feels* like they have become more detailed and more comprehensive, at least what comes to information and cyber security, at least in Finland, in the EU and in the US. For example, in the EU there is the General Data Protection Regulation (GDPR) (European Union, 2016). Network and Information Systems (NIS) regulation is about to make room for NIS2 (European Union, 2022). NIS2 will be applicable in late October 2024. Common nominators in GDPR and NIS2 is, for the organisations they concern, not meeting the requirements may mean that administrative fines will be sanctioned. As NIS2 is a directive, national adjustment is possible to perform. Time will tell whether there will be cyber security certification scheme or schemes which make it possible to participate to public bidding, for being compliant with NIS2 minimum or full cyber security requirements. For companies this could be interpreted as a carrot, instead of just currently existing administrative stick.

The U.S. Security and Exchange Commission (SEC) adopted rules on cybersecurity risk management in July 2023 “- - adopted rules requiring registrants to disclose material cybersecurity incidents they experience and to disclose on an annual basis material information regarding their cybersecurity risk management, strategy, and governance” (Securities and Exchange Commission, The, 2023). U.S. Food and Drug Administration (FDA) approved standards regarding network connectable components of health and welfare systems (2017; 2018), yet there are other FDA approved standards too. In the EU medical devices directive came applicable in 2021 (European Medicines Agency (EMA), 2021). With these samples It *seems* legislation and regulation have taken a position on at least procedural and technical cyber security.

## 3.3 Company’s Internal Responsibility

The investment and implementation of cyber security controls is dependent on the organisations internal risk management and assessment results, laws and regulations, and the business domains

specific requirements. Eventually, however, it is the organisations or company's sole internal decision how it protects and defends its assets, its value chain, and the value systems it is in. From business continuity perspective, it would be beneficial to have procedural, operation and technical (cyber) security controls in place, not only in a single organisation but in the whole ecosystem, or value system as Porter (1991) named it. When a (cyber) security control is triggered, other controls and the processes may be triggered. It is recommended that the controls and processes are exercised and trained. A *realistic enough* CA or CR is an excellent exercise environment for that.

## 3.4 What is a Cyber Range?

Cyber ranges are virtual or cyber-physical environments that are of many use-cases, and end-users. Cyber ranges are asymmetrically dependent on technologies: a cyber range must have technological platform, but a technological platform can exist without being utilised in a cyber range. Despite of the dependency and the over-evolving nature of technology in general, we are more interested the end-user point of view to CAs, CRs or CLs, and put technology in the side car.

The term *cyber range* initiates from military vocabulary and relates to physical world's *shooting range*. Both terms tip the intended usage in general, but do not describe the specifics. Wishing to understand better what a range offers is capable of; one must acquire more information. The listing of European cyber range platforms and solutions and a checklist by ECSO (2022), may be of great value for those of planning procuring a cyber range, as may be a similar kind of document by NIST/NICE Community Coordinating Council (2023). End-user organisations planning to invest in cyber range-based employee and management training service may find it beneficial, too, although some of checklist items are irrelevant in such cases; it may not in the interest of a service purchaser to know, what virtualisation technology is used. More focus and effort are probably put to develop and customise a one time or recurring service, which meets customer's requirements and expectations, not less *being realistic enough to provide the expected learning outcomes*.

In the physical world, shooting ranges differentiate based on capacity, capabilities, and other characteristics. The differentiating characteristics include the openness of the shooting range, the kinds of firearms that can be used, the person capacity of the range, and the facilities, services, and amenities the range, which limit or enable the events there can be organised. A range could be dedicated to security authorities only, or it could open for members of the area's shooting and

hunting club members and their guests. Some ranges could be targeted at Olympic trap, some for practical shooting. Larger ranges could include all the above mentioned, and several tracks for each activity. The realism the ranges and specific tracks offers to the attendees varies, naturally. For riffle calibre arms, there could be a still or a moving target, e.g., a silhouette of game running at the end of the track, to simulate game hunting and to train shooters aiming and shooting procedures. The largest scale shooting ranges, or areas, can offer a platform for joint military exercises and accommodate a very large number of participants from the various military domains, e.g., land, sea, air, and space. Or the domain representatives could be co-located, but the operational target area is shared. While shooting ranges are for developing and maintaining individuals' skills (*en masse*), shooting areas are mainly for organisations, either a single or multiple organisations simultaneously.

Cyber ranges that are more extensive e.g., in technological capabilities, capacity and features and functionalities may mimic the level of complexity of modern organisations' information and communications technology (ICT). Such cyber ranges could be named as *cyber arena*s (CAs)*,* as proposed by (Karjalainen & Kokkonen, 2020)As shooting ranges can be well-focused to specific kind of activity and audience, cyber ranges, too, can be well-focused and stay more-or-less static e.g., in terms of location and content offered to participants. Cyber ranges, due to their nature of being, at least partly, intangible, are understandably easier to modify or customise that their physical counterparts, shooting ranges.

For cyber ranges uses-cases Kick (2014) mentioned cyber exercise. Ferguson et al. (2014) listed six key steps, or use-cases, where a specific cyber range could be utilised: 1) understanding cybersecurity requirements, 2) characterizing the cyber-attack surface, 3) understanding the cyber kill chain, 4) perform tests to systems [in development, authors' note], following a framework's controls, 5) operational cyber vulnerability evaluation (to systems entering operational phase), 6) cyber operational resiliency evaluation, which is implemented simultaneously with training and exercises. NIST (2018) mentioned personnel assessment and certification, classroom education, competitions and exercises, global threat updated. ECSO (2020) mentioned several use-cases, including skills assessment, certification of products, persons, and processes. Several sources, including Švábenský et al. (2022), mention education. Organisations attending to cyber (range-based, authors' note) exercise must focus on impacts to critical systems and data (Kick, 2014).

Depending on the exercise, its financier, and the exercise's objectives, there may be several blue teams (BTs). Blue Teams are the target audience of CRXs an CLXs. BTs are formed by participants from a single or multiple organisations. Cyber range-based exercises *de facto* perform a hot washup where exercise participants, i.e., the blue teamers receive feedback about their performance. Usually, feedback is collected from all CRX participants, including but not limited to blue team members, that is. The feedback is gathered using survey tool or service. It is somewhat rare to perform a pre-survey, or pre-assessment to intended to-be CRX blue teamers on their expectations and wishes, as further is presented. To better understand the relationships of cyber range, its technical platform and cyber range-based events, a concept map is presented in the next chapter.

## 3.5 A Concept Map

As CAs, CRs and CLs are, at least to an extent, intangible, virtual, environments, persons new to idea may find it a bit difficult to understand. It has been suggested that utilising concept maps in corporate environments communication could be more effective, as they support learning and constructing knowledge (Starr & Parente de Oliveira, 2023). A concept map of cyber arena, cyber ranges, technical platforms, and events utilising CA an CR is presented in Figure 2. It distinguishes a cyber range from its technical platform and illustrates that a single cyber range-based event may, in fact, utilise several cyber ranges. A CR or its' technical platform may be distributed to several geographical or virtual locations. CR-based event participants may access the range, or it's technical platform, either from a specific physical location, or from an online location or both. In a cyber range-based event specific parts of the technical platform or the physical range can be offered to the audience, or the whole of those.

Each concept, a rounded rectangle with grey background, is in singular form. The linkage text between concepts tips about the cardinality between the concepts, but concrete instances of abstract concepts are coloured green. The relationship arrow direction tips the dependency direction. The presented concept map is neutral to virtualisation, emulation, and bare metal implementations, as it is neutral to physical network and virtual and tunnelled networks and a like. Respectively it is neutral to cyber-physical and full-virtual CRs.

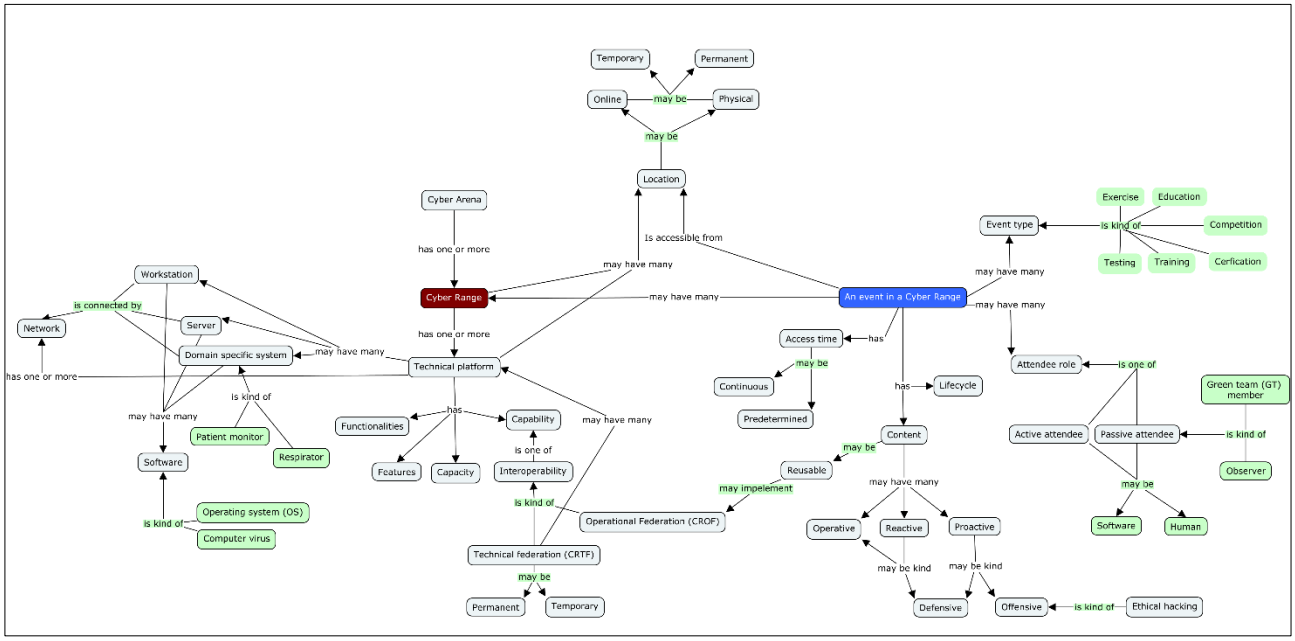


Figure 2: Cyber ranges relationship with cyber range-based events. Adopted from (Päijänen & Saharinen, 2022)

The concept map, made by the author, was initially presented in “Collection of agreements, guidance documentation and dissemination materials” by Päijänen & Saharinen (2022). It was created using CMapTools version 6.0.4 (The Institute for Human & Machine Cognition (IHMC), 2023). The concept map propositions are listed as text in Appendix 3 “Concept map Propositions as Text”, and they can be imported into CMapTools, as instructed in the appendix.

There is a strong relationship between a CR-based event location and the location of the CR. Due the current way of working, studying, etc., an event could be accessed online, on-site or hybrid. Similarly, the CR that the event utilises could be accessed from a specific physical location, from online access only, or hybrid. A CR-based event may utilise event contents that were initially used in another CR. This cyber range content re-use was called cyber range operational federation (CROF) (Suni, Piispanen, Nevala, Päijänen, & Saharinen, 2020). Arrangement where a CR utilises features, functionalities, capabilities, or capacity from another CR is called cyber range technical federation (CRTF) (Suni, Piispanen, Nevala, Päijänen, & Saharinen, 2020; Kokkonen, Sipola, Päijänen, & Piispanen, 2023). The presented concept map complements the cyber range taxonomy (Figure 3) authored by Yamin, Katt, & Gkioulos (2020), and supports understanding it.

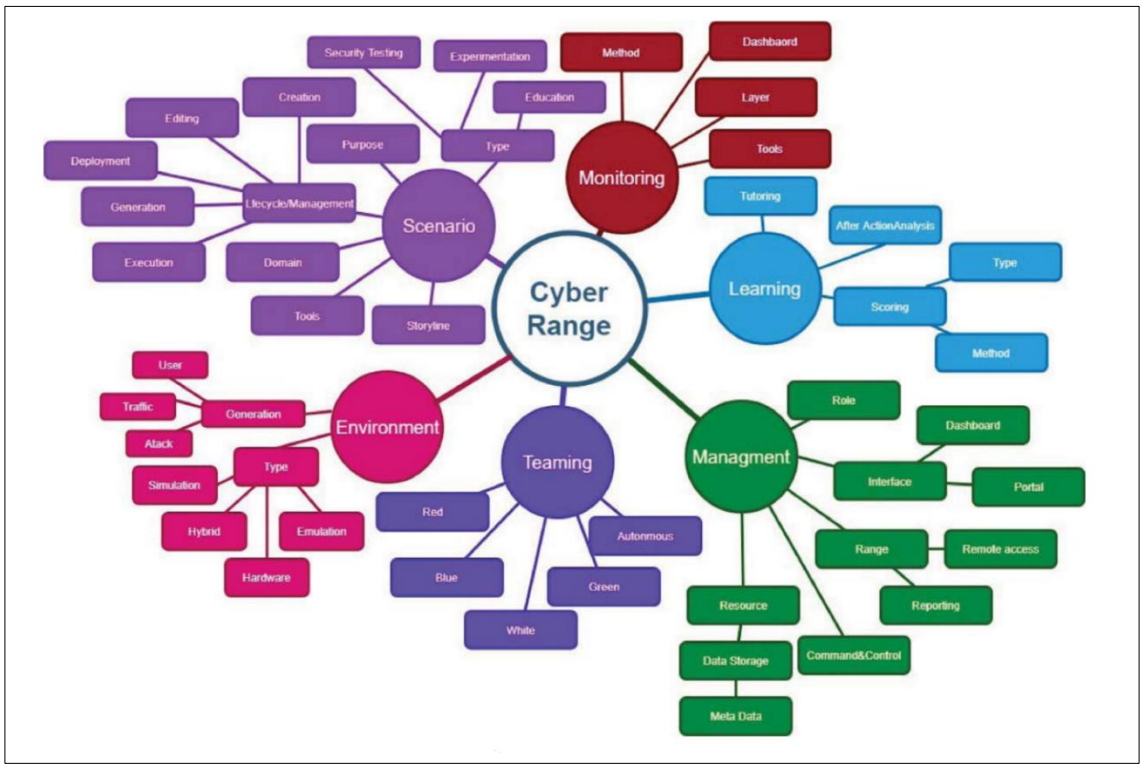


Figure 3: Cyber range taxonomy[1], authored by Yamin, Katt, & Gkioulos (2020)

Given an event in a cyber arena is defensive in nature, and its type is an exercise, then there are systems which a *blue team* should defend against the *red team* (Kick, 2014). Such target systems may be software-only like webservers, or cyber-physical systems such as commercial industrial automation (SCADA) or healthcare systems, like patient monitors and respirators. The cyber-physical systems can be considered as domain specific systems. The above-mentioned patient monitors and respirators are part of healthcare domain, thus are part of a healthcare cyber range, or the healthcare range of a cyber arena. The technical components, systems, software that form the technical platform of the cyber range are *network connected*, although some of them could be

[1] Reprinted from Computers & Security, vol. 88, Yamin, M. M., Katt, B., Gkioulos, V., Cyber ranges and security testbeds: Scenarios, functions, tools and architecture, Copyright (2020), with permission from Elsevier.

*network connectable*. Like in modern workplaces, remote employees' laptops may only occasionally communicate with employers' network and services therein. This kind of dynamic connectivity may give interesting exercise contents to blue teams.

Some CRs, or their technical platforms, can vary in their actual physical location. There are commercial CR operators, which have an entire cyber range movable within a truck container or trailer, e.g. IBM (2018) and WithSecure (2023). A cyber range technical platform could be set up temporally in varying location, given the hardware is in person movable racks, e.g. Airbus (2023) and Diateam (2023). The CR, in full or parts of, it could be in public cloud, or in private cloud in a datacentre. The concept map presented in Figure 2 can bend to the before mentioned alternative locations. Feedback about the figure was requested and received from author's own and project partners' colleagues. We highly appreciate the feedback. The presented map's concepts still need to be aligned with appropriate, existing taxonomies, for example with Cyber Taxi (Knüpfer, et al., 2020). However, there is room for taxonomy, ontology, and terminology development for what comes to CSs, CRs and CLs, as indicated by e.g., Karjalainen & Kokkonen (2020).

# 4 Literature Review

## 4.1 Data Search Plan

Used databases were IEEE Xplore (2023), Elsevier ScienceDirect (2023) and Google Scholar (2023). We had full-access licence to IEEE's service, and limited licence to Elsevier service. Google is open-accessible, but the indexed articles at the target databases could have required a licence, or some or all the articles therein could have been open-access. Planning the data search was an iterative process. The author's best interest was to acquire articles covering **cyber ranges and learning or training**, from the trainer or trainee perspective, but not e.g., machine learning or training an artificial intelligence solution with a dataset. Several rounds using the databases advanced search functional was taken. The possibilities that the databases offer to adjust search parameters, or to filter search results, varied. Did the database support setting additional query parameters or filter results, then those functionalities were used.

After several rounds, the timespan to collect particles was limited by setting article publication filter to 2022–2023 (as of writing it is 5 December 2023). The highly narrow timespan was due the

queries caused a lot of noise, i.e., results that were not of in authors' interests. By limiting the number of results, it was hoped to maximise the time to be used for analysis. Articles that were not available due licencing issues, or not being open access, were not taken included in the analysis.

**Attempt 1**

When limited articles publication years between 2020 – 2023, IEEE resulted three articles. No results were found from ScienceDirect. The queries used are below. Google Scholar's advanced search found three search results with query (with all the words) "Cyber Range" "pre-assessment" "pre-survey".

> **IEEE:** "Full Text & Metadata": "cyber range" AND ("Full Text & Metadata":"pre-assessment" OR "Full Text & Metadata":"pre-survey")
>
> **ScienceDirect:** "Cyber Range" AND ("pre-assessment" OR "pre-survey")

**Attempt 2**

For the second attempt, the terms joined by the OR operator, which is "pre-assessment" and "pre-survey" were replaced with "learning" and "training". The URL to replicate the queries is shown in Appendix 2.

**IEEE Xplore**

In IEEE's advanced command search the following query terms were used:

> "Abstract": "Cyber Range" AND ("Abstract ": "learning " OR " Abstract ": "training ")

After filters were applied, by limiting results to conferences and journals and setting the timespan between 2020-2023, total 16 articles were listed.

**Elsevier ScienceDirect**

ScienceDirect's advanced search was performed with year limit (2020-2023) and with the following search terms:

"Cyber Range" AND ("learning" OR "training")

The query resulted in total 102 articles.

**Google Scholar**

Google Scholar's advanced was used with search terms show below. Year limit was set to 2020-2023.

"Cyber Range" learning training

After the results appeared the option "Review articles" was selected. The Google Scholar search resulted 126 articles.

In total the queries resulted 224 articles. After this initial data search, it was considered that enough raw articles existed, so the search query and its parameters were transferred to a created small scripting utility, which was used to download the data.

## 4.2 Accepted Data Format

Instead of PDF-formatted articles, only articles available as HTML format were included. Rationale was that then contents of the articles could be technically analysed and handled with stock-Linux distribution tooling, i.e., by scripting. For data gathering a small Python version 3 language-based utility was created to assist interact with the databases and fetch the data. The utility was capable of handling IEEE Xplore' search functionality and walk through the search results, similarly to Elsevier's ScienceDirect search and Google Scholar's search and search results. Further, as Google only lists or indices articles available in other databases, the utility was modified to handle articles e.g.,

from mdpi.com, acm.com, etc. From the database provider point of, the script may behave similarly as a human user, although slightly faster but not much. The utility applied Microsoft's open-source Playwright library (Microsoft, 2023) to interact with the databases' user interfaces.

Data scraping (parsing) from text-formatted html is easy and straightforward. It is feasible to be performed on a light, consumer grade laptop. Data scraping, resulting good quality text-formatted data from PDF-files, however, is difficult. In fact, there are machine learning libraries that should assists with data scraping from PDFs, e.g., (Yupan, Tengchao, Lei, Yutong, & Furu, 2022) (Chen, Lv, Cui, Zhang, & Wei, 2022). The used utility approach was lighter than a ML/AI solution.

## 4.3 Data Analysis Process

The implemented utility was used to browse databases' search page, enter search terms and select query filters. The database specific result page URL was stored on the hard drive. The used result page URLs are listed in Appendix 2. During the initial manual search the author detected that each listed article was not accessible due to licensing issues. This was further better understood when the utility script was developed. Naïve logic was programmed into the utility; it checks whether certain words or phrases exists in the source [database] webpage. The used criteria are listed in Appendix 4. The utility script was used to download articles from the source databases.

After the download was finished, the number of articles was planned to be decreased by applying the common GNU Linux terminal commands, e.g., "*find*", "*grep*", "*awk*", "*sed*", "*sort*", "*uniq*", "*cut*", "*tr*", "*cat*" and "*cp*", applied in purpose created Bash shell scripts. The Linux distribution was based on Ubuntu 22.04 (jammy).

Using a purpose created Bash script, each article directory was assigned a technical identifier. Then technical analysis of data was pulled into a single comma separated value (csv) file, using another purpose created Bash script. The file was then opened in Microsoft Excel, where a human friendly identifier was assigned to each row. The Bash scripts are available at https://gitlab.com/janipaijanen/thesis-scripts.

Next was the first exclusion step. The used exclusion criteria are listed in Table 2. Fulfilment of any criteria in the set would have meant the specific article was no further processed. Criteria listed in

in Appendix 4 was used to determine if there was an access or not. If there was no access, then article-related license started with text “NOK”. Articles with access was indicated in the licence file with starting text “OK”. Survived abstracts, including the directory where the abstract file was, were copied under a new root directory.

Table 2: Exclusion criteria set #1

| No. | Exclusion Criteria |
|---|---|
| #1 | Database offers only a PDF file, but not article contents inside the HTML body |
| #2 | Access check indicates that no access exists (note: criteria is presented in Appendix 3) |
| #3 | No URL was recorded (due to the utility crash or other unexpected technical reason) |

After applying the exclusion criteria, 95 articles were excluded. There were then 67 articles to be reduced further. The used inclusion criteria are shown in Table 3.

Table 3: Inclusion criteria set #1

| No. | Inclusion Criteria |
|---|---|
| #1 | Article contents are available offline as plain text or html |
| #2 | Article abstract and title are available offline |
| #3 | Merged Title and Abstract fields contain “cyber range” and (“training” or “learning”) |

The filtering showed that download of 34 articles contents in text or HTML format were successful. However, from the total article set that survived the exclusion round to the inclusion round, only five articles fulfil the inclusion criteria #3.

## 4.4 Included Articles

The included five articles were “Security Scenarios Automation and Deployment in Virtual Environment using Ansible” (Acheampong, Bălan, Popovici, & Rekeraho, 2022), “A DNS-based Data Exfiltration Traffic Detection Method for Unknown Samples” (Ruiling, Jiawen, Xiang, & Shouyou, 2022), “Teaching Expert Development Project by KOSEN Security Educational Community” (Yonemura, et al., 2022), “Applying Process Discovery to Cybersecurity Training: An Experience Report” (Macak, Oslejsek, & Buhnova, 2022), and “Gamification of cyber ranges in cybersecurity education” (Jelo & Helebrandt, 2022).

**Security Scenarios Automation and Deployment in Virtual Environment using Ansible**

In the technical article Acheampong, Bălan, Popovici, & Rekeraho (2022), discuss their study about cloud orchestration technology, Ansible, which was used to setup a cloud based full-virtual CR. They list the (project) phases, which were a) design, b) implementation, c) automation and d) security scenarios, testing and evaluation. They managed to orchestrate and automate cyber range setup and configuration to cloud environment. They used virtual machines, that were pre-configured during the study. They report the results, where the commissioned cyber range is tested. The results Acheampong et al. achieved allow cost-effective, pay-per use approach-based cyber range, as the cyber range could be shut down when no users utilise it. When the need again rise, the applied technology setups and configures the environment to specified target state with minimal or no human interaction. Would the CR installation and configuration scripts be shared with other CR operators, then cyber range operational federation was implemented, which was shown in Figure 2 Based on our current understanding, CR operational federation (CROF) may work well, when the federation parties utilise about the same or exact technology and are about the equal in environment’s technical capacity and capability. A scenario, that may be avoidable in public clouds, is that CROF will face problems of the receiving CR’s technical platform are not near the capacity or capability of the sending/giving CR. This applies to private clouds or datacenters, but in public cloud en-

vironments one can choose, even programmatically the capacity and capabilities to be commissioned. In Kokkonen, et al. (2023) and Päijänen & Saharinen (2022) cyber range technical federation (CRTF) requirements were presented, and a demonstrator was reported. CRTF is a concept where CRs and alike can technically federate to other federation party's network to use the agreed CR features and functionalities. CRTF could relief CR investment pain, as CRs could specialize and the specialized features and functionalities could be used in CR-based events (Figure 2).While the Acheampong et al. paper was fundamentally technical, they mention that the deployed tools' [known, authors' note] vulnerablities are mapped against MITRE ATTT&CK framework (Mitre, 2023). Based on our experience, the mapping support learners, both students and existing professionals, as they are exposed to the graphcal, path-like, nature of threat actors tactics and techniques (and procedures, TTPs). Utilising MITRE's framework on the defensive side, may help reducing the possible next steps the attacker could do – which in turn could help the defender to perform reactive or proactive defensive maneurs. These kind of simulated scenarios could be exercised or trained in a cyber range, as indicated in Figure 2. Acheampong et al. mention the cyber security skills gap, naturally. They explicitly mention cyber security and IT professionals as possible end-user of the presented CR. Reframed to Porter's value stream (Figure 1), those roles would be located in Technoly support activity. Again, given the position of the paper, technical, it is highly understandable that the beforementioned professionals are considered as the target audience of the presented CR.

**A DNS-based Data Exfiltration Traffic Detection Method for Unknown Samples**

Advanved Persistent Threats (APTs) are state sponsored, or state related cyber threat actors. Usually they want to stay hidden in order to accomplish high reward offensive cyber operations. A known method that APTs use, is to exfiltrate data from an organisation via cover DNS channels. Should an organisation network work at expectly, DNS is required. It converts human understandable URLs to machine used IP-addresses. Ruiling et al. (2022) studied and propose a method, which in the study had detected on averated leakage of data in DNS traffic with over 99.925 % accuracy. The technical paper, reflected to Porter's value chain could some day be applied by IT and cyber security experts, positioning into support activies in the technology horizontal. The method presented in the study could be mapped into operations, a primary

activity. Given the lifecycle state of the technology, a better framework to be applied would be the innovation value chain (Hansen & Birkinshaw, 2007).

**Teaching Expert Development Project by KOSEN Security Educational Community**

Skills development of faculty members and KOSEN education community students were the objectives in (Yonemura, et al., 2022). The Japan-based authors mention the skills gap. They discuss the objectives the K-SEC project. Its secondary objective was to develop skills of students by quantitative methods, and the primary objective was to develop current students to cyber security professionals by qualitative methods. They illustrate a high-level schematic about utilising the faculty members' and students' knowledge, skills, and abilities (KSAs) in developing learning contents in cyber range-based education and training. They present analysis of pre- and post-training self-evaluation analysis which took place during a three-day Winter School. The analysis showed that learners KSAs had developed. The authors report that it is beneficial to conduct self-assessment before skills questionnaire at the beginning of a [CR, authors' note] lecture, and then based on data, adjust the knowledge delivery method of the lecture. Yonemura et. al discuss about education and training contents, and initial plans to increase the number of cyber ranges. As the faculty members were target users, then depending on the function they might fit to Technology (support activity) or Operations (primary activity) in the Porter's value chain. Rationale to fit into technology is that if faculity members are working with technology development, as they were, but also to Operations, as there are lecturers executing educationals' primary activity; lecturing. Developing young professionals with high cyber security KSAs provides value to KOSEN's value system, and KOSEN , too.

**Applying Process Discovery to Cybersecurity Training: An Experience Report**

Macak, Oslejsek, and Buhnova studied process discovery in cyber security training, specifically CTFs, by analysing sparse event log data (Macak, Oslejsek, & Buhnova, 2022). The report contains points to consider if such activity is tried, but also notes fundamental data cleaning steps, which eventually make the process discovery possible. They managed to perform process discovery: gather, cleanse, and connect the log data and represent it in directed graph way. They noticed that the graphical representation was difficult and should be researched further. The authors wonder,

which would be more intuitive presentation media: a static 2D-presentation, or interactive 3D model. Both are difficult to implement. The presented process mining could benefit both learners and lecturers or trainers. As the behaviour of learners could be automatically presented in graphical form, determining which skills and abilities areas could be improved [and if knowledge gaps exist, authors' note]. Macak et al. noted that only a few papers addressed cyber security learning.

**Gamification of cyber ranges in cybersecurity education**

Jelo and Helebrandt (Jelo & Helebrandt, 2022) emphasized CR-based training and education should be close to real-world, and gamified. They note that gamification is a way to motivate students in cyber security, and that learning by doing, or hands-on learning is the best way to remember and learn. Jelo and Helebrandt reported a fully functional and self-contained CTF-based game as the main contribution of their paper. Jelo and Helebrandt state that they used Masaryk University published, and open-source, Cyber Sandbox Creator (CSC) to create the game. The learners exposed the CTF reported they learnt new skills, abilities, or knowledge.

Authors commented that the Jelo and Helebrandt published CTF-based game can be seen to trying to reduce the skills gap. Since the game was offensive by its nature, there is a concern on one's domestic legislation: does it allow offensive learning or training except for dedicated institutions or organisations? As we indicated earlier, legislation and regulation have evolved, and we estimate it will evolve globally; it will be more detailed and more comprehensive. A question is will that developed legislation be more enabling or disabling for what comes develop offensive skills. However, to defend organisation's assets well, it has been said to be beneficial to understand how threat actors exploit vulnerabilities and weaknesses in the deployed software and systems, and in organisation's controls. Mapping Jelo and Helebrandt's reported CTF to Porter's value chain, we place it on operations, a primary activity.

The included papers do not indicate explicitly how cyber range-based exercise content needs are enquired from participants before the reported exercise(s). Jelo and Helebrandt (2022), and Macak, et al. (2022), Yonemura, et al. (2022), and Acheampong, et al. (2022), reported their backgrounds in academia or education. It could be that contents and exercise objectives are given to

learners and stated in curriculum. Their papers support or describe solutions that support bridging the skills gap.

# 5 Complementary Conclusions and Further Ideas

Several referenced papers stated that hands-on, or hands on handles training works best for what comes to cyber security education and training. In our article we reported that cyber range- and cyber lab-based exercise participants preferred technical contents over non-technical contents. Simultaneously while enquiring the participants needs and wishes, we reported that the used pre-survey itself was evaluated. The results indicate that the survey can be used similarly in the future, prior to exercises, to gain better customer, or participant, understanding. In the conducted self-assessment of research's ethicality and reliability we reported that there was potential bias in the survey setup, as survey respondents had already registered to cyber range- or cyber-lab-based event, and they knew that there would be technical contents. Had the survey source group be selected differently and had the survey's multi-choice options order been randomised, there could have been other kind of survey results. More research is needed to understand the needs of CRXs and CLXs participants needs and wishes, and in addition to remove potential bias.

There is global need of skilled cybersecurity professionals and those, who in their daily duties, need to understand and apply cybersecurity. Means to supply the need of such professionals were reported to be through the education system, and reskilling and upskilling existing professionals. Three of five articles that were included in the literature review directly support cyber professionals supply, either by education system, or training in cyber range- or cyber-lab-based exercises and trainings. Sources report that organisations and companies utilise cyber ranges for exercising. We reported that organisations various cyber security controls and processes can be exercised, and that the implications of exploiting such could be experienced in a CRX. To support cyber range service or technology buyers, we noted two distinct cyber range listings, one by ECSO and another by NICE. In general to support understanding the relationship between cyber range-based events and cyber ranges and the technical platforms used, we represented a concept map in Figure 2. The concept map could be further joint-developed, to support the development of cyber range-based taxonomy and terminology. We noticed the asymmetric relationship between a cyber range and its one or more technical platforms: a cyber range must have at least one technical platform, but a technical platform can exist without being used in a cyber range.

Not only does technology evolve, but regulation and legislation *seem* to do that too. We listed a few examples of EU and US legislation and regulation that are or will be effective within the next calendar year, that is by the end of 2024. In the EU NIS2 will enforce critical infrastructure companies to take actions and look after their most critical supply chain. The situation with NIS2 will be and with general data protection regulation (GDPR) it is, that instead of carrot, only stick is available, as if critical infrastructure company fail to comply, then administrative fines are condemned. In the US the Stock Exchange Commission (SEC) have set requirements to public listed companies' cyber security. This provides high demand for business executives to understand cyber security basics, and cyber security professionals to understand the fundamental concept of company's strategy expressed, e.g., by Porter.

In the conducted narrative-systematic literature review we tried to understand how participants' learning needs, objectives or priorities were considered in planning cyber range-based exercises, and how does literature indicate that Porter's value chain has been applied when participating organisations selected participants to a cyber range-based exercise. Using the reported process and exclusion and inclusion criteria, five articles were included in the research. The starting point was 224 articles in total. The data gathering process is documented and it is reproducible. By applying Porter's theory of value chain, we also wanted to highlight that cyber security professionals *must* understand the basic concept of company's strategy. In addition, we wanted to highlight that business strategists, decision makers and students alike *must* understand that cyber security cover each company's and organisation's all primary and support activities, and that cyber security can be exercised in cyber range-based exercises. A cyber-attack may have severe consequences in a company and its value chain. Or worse yet, a cascading effect exploiting vulnerabilities or weaknesses of a company may have very serious consequences not only in the digital interconnected business networks but in physical world of the company's value system. In short, we want to bring cyber security and business decision makers closer to together.

The lack of support from the literature for the research questions indicate that the primary and supportive research question were not answered. More research is needed on the subject. There are indicators that organisations and companies seizing cyber range-based events, to develop their employees, refrain to disclose information of participation, at least in the white literature. On the other hand, it is understandable that the information is not disclosed. By doing so, organisations

and companies execute their operational security and risk assessment procedures. In the future, more systematic and broader research, and including the grey literature, could be performed.

# References

Acheampong, R., Bălan, T. C., Popovici, D. -M., & Rekeraho, A. (2022). Security Scenarios Automation and Deployment in Virtual Environment using Ansible. *2022 14th International Conference on Communications (COMM).* doi:10.1109/COMM54429.2022.9817150

Airbus. (2023). CyberRange. Retrieved December 4, 2023, from https://www.cyber.airbus.com/cyberrange/

Bloom, B. e. (1956). Taxonomy of Educational Objectives - The Classification of Educational Goals. London:: Longmans, Green and Co Ltd.

Booth, A., Briscoe, S., & Wright, J. M. (2020). The "realist search": A systematic scoping review of current practice and reporting. *Research, 11*(1), 14-35. doi:10.1002/jrsm.1386

Brookson, C., Cadzow, S., Eckmaier, R., Eschweiler, J., Gerber, B., Guarino, A., . . . Górniak, S. (2015, December). Definition of Cybersecurity. (1.0). EU: European Union Agency for Network and Information Security (ENISA). doi:10.2824/4069

Cebula, J. J., Popeck, M., & Young, L. R. (2014, May 21). A Taxonomy of Operational Cyber Security Risks Version 2. (Technical Note CMU/SEI-2014-TN-006). doi:https://doi.org/10.1184/R1/6571784.v1

Centre for Science and Technology Studies, Leiden University. (2023). *Features*. Retrieved September 10, 2023, from VOSViewer: https://www.vosviewer.com/features/highlights

Chen, J., Lv, T., Cui, L., Zhang, C., & Wei, F. (2022). XDoc: Unified Pre-training for Cross-Format Document Understanding. *arXiv preprint arXiv:2210.02849*. Retrieved December 6, 2023, from https://arxiv.org/abs/2210.02849

Collins, J. A., & Fauser, B. C. (2005, March/April). Balancing the strengths of systematic and narrative reviews. *Human Reproduction Update, 11*(2), 103-104. doi:https://doi.org/10.1093/humupd/dmh058

Council of the European Union. (2017). Council Recommendation on European Qualifications Framework for lifelong. Retrieved December 4, 2023, from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32017H0615(01)&from=EN

Coutinho, S., Bollen, A., Weil, C., Sheerin, C., Silvera, D., Donaldson, S., & Rosborough, J. (2023). *Cyber security skills in the UK labour market 2023.* Department for Science, Innovation and Technology. Ipsos. Retrieved December 02, 2023, from https://assets.publishing.service.gov.uk/media/64be95f0d4051a00145a91ec/Cyber_security_skills_in_the_UK_labour_market_2023.pdf

CyberSecurity & Infrastructure Security Agency (CISA). (2021, Janurary 7). Supply Chain Compromise. Retrieved December 4, 2023, from https://www.cisa.gov/news-events/alerts/2021/01/07/supply-chain-compromise

CyberSeek. (2023, 12 03). *Heatmap.* Retrieved 12 03, 2023, from CyberSeek: https://www.cyberseek.org/heatmap.html

CyBOK. (2021, July). Cyber security Body of Knowledge (CyBOK). (v1.1). University of Bristol. Retrieved December 6, 2023, from https://www.cybok.org/knowledgebase1_1/

DIATEAM. (2023). WHAT'S A CYBER RANGE? Retrieved December 4, 2023, from https://www.diateam.net/what-is-a-cyber-range/

Disis, J., & Mahmood, Z. (2021, May 28). Microsoft says SolarWinds hackers have struck again at the US and other countries. CNN Business. Retrieved December 4, 2023, from https://edition.cnn.com/2021/05/28/tech/microsoft-solarwinds-russia-hack-intl-hnk/index.html

ECSO. (2020, March 14). Understanding Cyber Range: From Hype to Reality. Retrieved 12 01, 2023, from https://ecs-org.eu/?publications=https-ecs-org-eu-documents-publications-5fdb291cdf5e7-pdf

Elsevier. (2023). *ScienceDirect*. Retrieved from https://www.sciencedirect.com

European Commission. Joint Research Centre. (2019). A proposal for a European cybersecurity taxonomy. doi:https://data.europa.eu/doi/10.2760/106002

European Cyber Security Organisation, ECSO. (2022, December 12). Cyber Range Features Checklist & List of European Providers. (2022 Edition). (E. WG5, Ed.) Brussels, Belgium. Retrieved 12 01, 2023, from https://ecs-org.eu/?publications=cyber-range-features-checklist

European Medicines Agency (EMA). (2021, May 26). Medical Device Regulation comes into application. Retrieved December 4, 2023, from https://www.ema.europa.eu/en/news/medical-device-regulation-comes-application

European Union (EU). (2023, September 14). *CyberSec4Europe.* doi:https://doi.org/10.3030/830929

European Union. (2016, April 27). General Data Protection Regulation. Retrieved December 4, 2023, from Regulation (EU) 2016/679

European Union. (2022, December 14). Measures for a high common level of cybersecurity across the Union, NIS2 Directive. Retrieved December 4, 2023, from https://eur-lex.europa.eu/eli/dir/2022/2555

European Union Agency for Cybersecurity (Enisa). (2023, September 21). *Cybersecurity Skills Conference: Strengthening human capital in the EU.* Retrieved December 03, 2023, from Enisa News: https://www.enisa.europa.eu/news/cybersecurity-skills-conference-strengthening-human-capital-in-the-eu

Ferguson, B., Tall, A., & Olsen, D. (2014). National Cyber Range Overview. *2014 IEEE Military Communications Conference* (pp. 123-128). Baltimore, MD, USA: IEEE. doi:10.1109/MILCOM.2014.27

Finnish Broadcasting Company. (2021, January 5). *HS: Vastaamo's new owners make police complaint over purchase*. Retrieved September 03, 2023, from YLE News: https://yle.fi/a/3-11725388

Finnish Broadcasting Company. (2022, July 20). Probe of psychotherapy firm's data breach finds possible European, employee links. Finland: YLE. Retrieved September 03, 2023, from https://yle.fi/a/3-12543823

Finnish Broadcasting Company. (2023, August 31). *NBI completes investigation into psychotherapy centre hacking, extortion*. Retrieved September 03, 2023, from YLE News: https://yle.fi/a/74-20047972

Finnish Broadcasting Company. (2023a, April 18). *Hacked therapy centre's ex-CEO gets 3-month suspended sentence*. Retrieved September 03, 2023, from YLE News: https://yle.fi/a/74-20027665

Food and Drug Administration (FDA). (2018, July 06). Recognized Consensus Standards: Medical Devices. *Standard for Safety, Software Cybersecurity for Network-Connectable Products, Part 2-1: Particular Requirements for Network Connectable Components of Healthcare and Wellness Systems*. Retrieved December 4, 2023, from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/detail.cfm?standard__identification_no=37046

Food and Drug Administration. (2017, August 21). Recognized Consensus Standards: Medical Devices. *Standard for Safety, Standard for Software Cybersecurity Network-Connectable Products, Part 1: General Requirements*. Retrieved December 4, 2023, from https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/detail.cfm?standard__identification_no=36149

Google. (2023). *Google Scholar*. Retrieved from https://scholar.google.com/

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal, 26*(2), 91-108. doi:10.1111/j.1471-1842.2009.00848.x

Greenberg, A. (2018, August 18). The Untold Story of NotPetya, the Most Devastating Cyberattack in History. Wired. Retrieved December 04, 2023, from https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

Greenhalgh, T., Thorne, S., & Malterud, K. (2018, June). Time to challenge the spurious hierarchy of systematic over narrative reviews. *European journal of clinical investigation, 48*(6). doi:doi:10.1111/eci.12931

Hansen, M., & Birkinshaw, J. (2007, June). Innovatoin Value Chain. Harward Business Review. Retrieved December 6, 2023, from https://hbr.org/2007/06/the-innovation-value-chain

Hoffman, L., Rosenberg, T., & Dodge, R. (2005). Exploring a national cybersecurity exercise for universities. *IEEE Security & Privacy*, 27-33. doi:10.1109/MSP.2005.120

HSE. (2021, December 10). *HSE publishes independent report on Conti cyber attack*. Retrieved September 03, 2023, from Health Service Executive: https://www.hse.ie/eng/services/news/media/pressrel/hse-publishes-independent-report-on-conti-cyber-attack.html

IBM Plc. (2018, November 5). IBM X-Force Command Experience – Cyber Security training on wheels. Retrieved December 4, 2023, from https://www.ibm.com/blogs/nordic-msp/ibm-x-force/

IEEE. (2023). *IEEE Xplore*. Retrieved from https://ieeexplore.ieee.org/Xplore/home.jsp

Ivančić, L., Glavan, L., & Vukšić, V. (2020). A Literature Review of Digital Transformation in Healthcare. *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)* (pp. 1351-1355). Opatija: IEEE. doi:10.23919/MIPRO48935.2020.9245259

Jelo, M., & Helebrandt, P. (2022). Gamification of cyber ranges in cybersecurity education. *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, (pp. 280-285). doi:10.1109/ICETA57911.2022.9974714

JYVSECTEC. (2022). *Cyber Range Overview.* Retrieved December 3, 2023, from Jyvsectec: https://jyvsectec.fi/rgce

Karinsalo, A., & Halunen, K. (2021, June). Design of Education and Professional Framework. CyberSec4Europe. Retrieved December 4, 2023, from https://cybersec4europe.eu/wp-content/uploads/2021/06/D6_3_Design-of-Education-and-Professional-Frame-work_Final.pdf

Karinsalo, A., Saharinen, K., Päijänen, J., & Salonen, J. (2022). Pedagogical and self-reflecting approach to Improving the Learning Within a Cyber Exercise. *Proceedings of the European conference on cyber*, *21(1)*, pp. 105-114. doi:10.34190/eccws.21.1.221

Karjalainen, M. (2021, June 9). Pedagogical Basis of Live Cybersecurity Exercises. *JYU dissertations*. Retrieved 12 04, 2023, from http://urn.fi/URN:ISBN:978-951-39-8738-1

Karjalainen, M., & Kokkonen, T. (2020). Comprehensive Cyber Arena; The Next Generation Cyb. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 11-16). [Online]: IEEE. doi:10.1109/EuroSPW51379.2020.00011

Kick, J. (2014, November 15). *Cyber Exercise Playbook.* Retrieved September 03, 2023, from Mitre: https://www.mitre.org/news-insights/publication/cyber-exercise-playbook

Kitchenham, B., Brereton, P., Li, Z., Budgen, D., & Burn, A. (2011). Repeatability of systematic literature reviews. *15th Annual Conference on Evaluation & Assessment in Software Engineering (EASE 2011)* (pp. 46-55). Durham: IET. doi:10.1049/ic.2011.0006

Knüpfer, M., Bierwirth, T., Stiemert, L., Schopp, M., Seeber, S., Pöhn, D., & Hillmann, P. (2020). Cyber Taxi: A Taxonomy of Interactive Cyber Training and Education Systems. In G. Hatzivasilis, & S. Ioannidis (Ed.), *Model-driven Simulation and Training Environments for Cybersecurity. MSTEC 2020. Lecture Notes in Computer Science. vol 12512*, pp. 3-21. Springer, Cham. doi:10.1007/978-3-030-62433-0_1

Kokkonen, T., Päijänen, J., & Sipola, T. (2023). Multi-National Cyber Security Exercise, Case Flagship 2. *Proceedings of the 14th International Conference on Education Technology and Computers. ICETC '22*, pp. 292–298. Association for Computing Machinery. Retrieved December 3, 2023, from https://doi.org/10.1145/3572549.3572596

Kokkonen, T., Sipola, T., Päijänen, J., & Piispanen, J. (2023). Cyber Range Technical Federation: Case Flagship 1 Exercise. In T. Dimitrakos, J. Lopez, & F. Martinelli (Eds.), *Collaborative Approaches for Cyber Security in Cyber-Physical Systems. Advanced Sciences and Technologies for Security Applications.* Springer, Cham. doi:https://doi.org/10.1007/978-3-031-16088-2_1

Kuluttajaliitto. (2020, October 26). Neuvoja tietovuodon kohteeksi joutuneille (in Finnish). Retrieved September 03, 2023, from https://www.kuluttajaliitto.fi/blog/2020/10/26/neuvoja-tietovuodon-kohteeksi-joutuneille/

Langner, G., Skopik, F., Furnell, S., & Quirchmayr, G. (2022). A Tailored Model for Cyber Security Education Utilizing a Cyber Range. *Proceedings of the 8th International Conference on Information Systems Security and Privacy - ICISSP* (pp. 365-377). SciTePress. doi:10.5220/0010834000003120

Lee, L. (2019). Cybercrime has evolved: it's time cyber security did too. *Computer Fraud & Security, 2019*(6), 8-11. doi:https://doi.org/10.1016/S1361-3723(19)30063-6

Lehto, M. (Ed.). (2022, September 08). Kyberturvallisuuden koulutusohjelman muutostarpeiden tutkimus – hankkeen loppuraportti. Jyväskylän yliopisto, Informaatioteknologian tiedekunta. Retrieved December 02, 2023, from https://jyx.jyu.fi/bitstream/handle/123456789/82709/Kyberturvallisuuden%20koulutusohjelman%20muutostarpeiden%20tutkimus%20v4.pdf?sequence=1&isAllowed=y

Macak, M., Oslejsek, R., & Buhnova, B. (2022). Applying Process Discovery to Cybersecurity Training: An Experience Report. *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, (pp. 394-402). doi:10.1109/EuroSPW55150.2022.00047

Microsoft. (2023). Playwright for Python. Retrieved December 6, 2023, from https://playwright.dev/python/

Mitre. (2023). MITRE ATT&CK framework. Retrieved December 6, 2023, from https://attack.mitre.org/

MTV Uutiset. (2022, June 06). *MTV:n tiedot: Tapioiden perhe tuomittiin miljoonakorvauksiin Vastaamosta*. Retrieved September 03, 2023, from MTV Uutiset: https://www.mtvuutiset.fi/artikkeli/mtv-n-tiedot-tapioiden-perhe-tuomittiin-miljoonakorvauksiin-vastaamon-ostanut-yritys-saa-rahansa-takaisin-vaikenee-tilanteesta-taysin/8445892

Musunuru, K. (2021, June 10). litreviewer: A Python Package for Review of Literature (RoL). Social Science Research Network. Retrieved September 10, 2023

National Audit Office. (2017, October 27). *Investigation: WannaCry cyber attack and the NHS*. Retrieved September 03, 2023, from Nation Audit Office: https://www.nao.org.uk/reports/investigation-wannacry-cyber-attack-and-the-nhs/

National Bureau of Investigation. (2023, August 31). *Criminal investigation into Vastaamo hacking case completed*. Retrieved September 03, 2023, from Police of Finland: https://poliisi.fi/en/-/criminal-investigation-into-vastaamo-hacking-case-completed

National Institute of Standards and Technology (NIST). (2018, February 13). Cyber Ranges. Retrieved December 01, 2023, from https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf

National Institute of Standards and Technology (NIST). (n.d.). *Operations Security.* Retrieved December 03, 2023, from Computer Security Resource Center: https://csrc.nist.gov/glossary/term/operations_security

National Institute of Standards and Technology (NIST). (n.d.). *Technical Controls.* Retrieved December 03, 2023, from Computer Security Resource Center: https://csrc.nist.gov/glossary/term/technical_controls

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017, August). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. National Institute of Standards and Technology (NIST). doi:https://doi.org/10.6028/nist.sp.800-181

NICE Community Coordinating Council. (2023, 09). The Cyber Range: A Guide. NIST/NICE. Retrieved December 2, 2023, from https://www.nist.gov/document/cyber-range

Nurse, J. R., Adamos, K., Grammatopoulos, A., & Franco, F. D. (2021). Addressing the EU Cybersecurity Skills Shortage and Gap Through Gigher Education. European Union Agency for Cybersecurity (ENISA). doi:10.2824/033355

Päijänen, J., & Saharinen, K. (2022, June 30). Collection of agreements, guidance documentation and dissemination materials. CyberSec4Europe. Retrieved 12 01, 2023, from CyberSec4Europe: https://cybersec4europe.eu/wp-content/uploads/2022/07/D7.6-Collection-of-agreements-guidance-documentation-and-dissemination-materials-v1_0_submitted-1.pdf

Päijänen, J., Piispanen, J., & Viinikanoja, J. (2022). Flagship 2. CyberSec4Europe. Retrieved December 1, 2023, from https://cybersec4europe.eu/wp-content/uploads/2022/04/D6.5-Flagship-2-v1.3_submitted.pdf

Päijänen, J., Saharinen, K., Salonen, J., SIpola, T., Vykopal, J., & Kokkonen, T. (2022). Cyber Range – Preparing for Crisis or Something Just for Technical People? In T. Eze, L. Speakman, & C. Onwubiko (Ed.), *Proceeding of the 20th European Conference on Cyber Warfare and Security ECCWS 2021. 21*, pp. 322-331. [Online]: Academic Conferences International. doi:https://doi.org/10.34190/EWS.21.012

Päijänen, J., Salonen, J., Karinsalo, A., Sipola, T., & Kokkonen, T. (2023). Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones. *Proceedings of the 22nd European Conference on Cyber Warfare and Security. 22*, pp. 349-357. [Online]: Academic Conferences International Limited. doi:https://doi.org/10.34190/eccws.22.1.1196

Päijänen, J., Viinikanoja, J., & Piispanen, J. (2021). Flagship 1. CyberSec4Europe. Retrieved December 1, 2023, from https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5da129648&appId=PPGMS

Palmatier, R. W., Houston, M. B., & Hulland, J. (2018). Review articles: purpose, process, and structure. *Journal of the Academy of Marketing Science*, 1-5. doi:10.1007/s11747-017-0563-4

Petersen, R., Santos, D., Wetzel, K. A., Smith, M. C., & Witte, G. (2020, November). Workforce Framework for Cybersecurity (NICE Framework). (NIST Special Publication 800-181 Revision 1). doi:https://doi.org/10.6028/NIST.SP.800-181r1

Pimentel, J. F. (2022). *Snowballing.* Retrieved September 10, 2023, from github: https://github.com/JoaoFelipe/snowballing

Pluralsight LLC. (2023). State of Upskilling 2023. Retrieved February 02, 2023, from https://www.pluralsight.com/resource-center/state-of-upskilling-2023

Porter, M. E. (1991). Towards a Dynamic Theory of Strategy. *Strategic Management Journal, 12*(52), 95-117. doi:https://doi.org/10.1002/smj.4250121008

Renner, A., Müller, J., & Theissler, A. (2022). State-of-the-art on writing a literature review: An overview of types and components. *2022 IEEE Global Engineering Education Conference (EDUCON)* (pp. 1895-1902). Tunis: IEEE. doi:10.1109/EDUCON52537.2022.9766503

Ruiling, G., Jiawen, D., Xiang, C., & Shouyou, S. (2022). A DNS-based Data Exfiltration Traffic Detection Method for Unknown Samples. *2022 7th IEEE International Conference on Data Science in Cyberspace (DSC)*, (pp. 191-198). doi:10.1109/DSC55868.2022.00032

Securities and Exchange Commission, The. (2023, July 26). SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies.

Washington D.C., US. Retrieved December 4, 2023, from https://www.sec.gov/news/press-release/2023-139

Snyder, H. (2019, September). Literature review as a research methodology: An overview and guidelines. *Journal of Business Research, 104*, 333-3339. doi:10.1016/j.jbusres.2019.07.039

Starks, T. (2023, October 30). SEC: SolarWinds failed to disclose cybersecurity woes before historic breach. Washington Post, the. Retrieved December 4, 2023, from SEC: SolarWinds failed to disclose cybersecurity woes before historic breach

Starr, R. R., & Parente de Oliveira, J. M. (2023). Concept maps as the first step in an ontology construction method. *Information Systems*, 771-783. doi:https://doi.org/10.1016/j.is.2012.05.010

Suni, E., Piispanen, J., Nevala, J., Päijänen, J., & Saharinen, K. (2020, September). Report on existing cyber ranges, requirements. CyberSec4Europe. Retrieved 12 03, 2020, from https://cybersec4europe.eu/wp-content/uploads/2020/09/D7.1-Report-on-existing-cyber-ranges-and-requirement-specification-for-federated-cyber-ranges-v1.0_submitted.pdf

Švábenský, V., Weiss, R., Cook, J., Vykopal, J., Čeleda, P., Mache, J., . . . Chattopadhyay, A. (2022). Evaluating Two Approaches to Assessing Student Progress in Cybersecurity Exercises. *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education - Volume 1. SIGCSE 2022*, pp. 787-793. New York, NY, USA: Association for Computing Machinery. doi:10.1145/3478431.3499414

The Institute for Human & Machine Cognition (IHMC). (2023, 10 19). *CMapTools download page*. Retrieved from https://cmap.ihmc.us/cmaptools/

The Office of the Data Protection Ombudsman. (2020, October 25). Advice for the victims of the data leak. Finland. Retrieved September 03, 2023, from https://tietosuoja.fi/-/neuvoja-tietovuodon-kohteeksi-joutuneille?languageId=en_US

The Office of the Data Protection Ombudsman. (2021, December 16). Administrative fine imposed on psychotherapy centre Vastaamo for data protection violations. Finland. Retrieved September 03, 2023, from https://tietosuoja.fi/en/-/administrative-fine-imposed-on-psychotherapy-centre-vastaamo-for-data-protection-violations

The Security Committee. (2018). Vocabulary of Cyber Security. Helsinki, Finland: The Finnish Terminology Centre. Retrieved September 3, 2023, from https://turvallisuuskomitea.fi/kyberturvallisuuden-sanasto/

Tieteen Termipankki. (2021, June 23). Narratiivinen katsaus. Retrieved December 6, 203, from https://tieteentermipankki.fi/wiki/Tiedeneuvonta:narratiivinen_katsaus

Turnbull, D., Chugh, R., & Luck, J. (2023, January 1). Systematic-narrative hybrid literature review: A strategy for integrating a concise methodology into a manuscript. *Social Sciences & Humanities Open*, 100381. doi:https://doi.org/10.1016/j.ssaho.2022.100381

Valvira. (2021, May 19). Psykoterapiakeskus Vastaamo Oy laiminlöi useita velvollisuuksiaan (in Finnish). Retrieved September 03, 2023, from https://www.valvira.fi/-/psykoterapiakeskus-vastaamo-oy-laiminloi-useita-velvollisuuksiaan

van Eck, N., & Waltman, L. (2015, February 16). Introduction to VOSviewer. Leiden: Youtube. Retrieved September 10, 2023, from https://youtu.be/9dTWkNRxUtw

Vilkka, H. (2023). *Kirjallisuuskatsaus metodina, opinnäytetyön osana ja tekstilajina.* Art House.

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P., & Tovarnak, D. (2017). Lessons learned from complex hands-on defence exercises in a cyber range. *2017 IEEE Frontiers in Education Conference (FIE)*, (pp. 1-8). doi:10.1109/FIE.2017.8190713

Wang, L., Tian, Z., & Gu, Z. L. (2019). Crowdsourcing Approach for Developing Hands-On Experiments in Cybersecurity Education. *IEEE Access, 7*, 169066-169072. doi:10.1109/ACCESS.2019.2952585

WithSecure Plc. (2023). WithSecure Cyber Tour. Retrieved December 4, 2023, from https://www.withsecure.com/en/expertise/campaigns/cybertour

Wolfenden, B. (2019). Gamification as a winning cyber security strategy. *Computer Fraud & Security*(5), 9-12. doi:https://doi.org/10.1016/S1361-3723(19)30052-1

World Economic Forum. (2022, May 2). *The cybersecurity skills gap is a real threat - here's how to address it.* Retrieved December 03, 2023, from World Economic Forum / Davos Agenda: https://www.weforum.org/agenda/2023/05/the-cybersecurity-skills-gap-is-a-real-threat-heres-how-to-address-it/

Yamin, M. M., Katt, B., & Gkioulos, V. (2020, January). yber ranges and security testbeds: Scenarios, functions, tools and architecture. (Computers & security). Elsevier. doi:https://doi.org/10.1016/j.cose.2019.101636

Yonemura, K., Oyama, S., Kobayashi, H., Yamada, S., Shiraishi, K., Izumi, S., . . . Kishimoto, S. (2022). Teaching Expert Development Project by KOSEN Security Educational Community. *022 IEEE Global Engineering Education Conference (EDUCON)*, (pp. 1643-1651). doi:10.1109/EDUCON52537.2022.9766560

Yupan, H., Tengchao, L., Lei, C., Yutong, L., & Furu, W. (2022). LayoutLMv3: Pre-training for Document AI with Unified Text and Image Masking. *Proceedings of the 30th ACM International Conference on Multimedia. MM '22*, pp. 4083–4091. Lisboa, Portugal: Association for Computing Machinery. doi:10.1145/3503161.3548112

# Appendices

## Appendix 1. Research Article

Päijänen, J., Salonen, J., Karinsalo, A., Sipola, T., & Kokkonen, T. (2023).

### Participants Prefer Technical Hands-on Cyber Exercises Instead of Organisational and Societal Ones

**Jani Päijänen[1], Jarno Salonen[2], Anni Karinsalo[2], Tuomo Sipola[1] and Tero Kokkonen[1]**
[1]Institute of Information Technology, Jamk University of Applied Sciences, Jyväskylä, Finland
[2]VTT Technical Research Centre of Finland, Espoo, Finland

jani.paijanen@jamk.fi
jarno.salonen@vtt.fi
anni.karinsalo@vtt.fi
tuomo.sipola@jamk.fi
tero.kokkonen@jamk.fi

**Abstract:** The current shortage of cybersecurity professionals is about 2 million people worldwide, and in Europe the industry is seeking for about 350 000 skilled professionals. There is also an enormous need for dedicated cybersecurity training courses for existing professionals who wish to acquire completely new skills or maintain their current ones. Due to the lack of new skilled workforce, the current cybersecurity personnel are overworked in their work. In order not to waste the valuable time of cybersecurity professionals with unnecessary training, cyber exercises should be well prepared. This article is based on research conducted in a European collaborative project and more specifically, a cyber exercise organised in early 2022. The purpose of our research was to conduct a preliminary assessment of the participants to learn about their skills and expectations before the cyber exercise. This assessment was used for fine-tuning the exercise. To achieve this, we identified common trends in the participants' interests during the cyber exercise. The preliminary assessment was carried out as a web survey. The responses were cross tabulated to find meaningful indicators related to skills and interests of the participant group. We identified the most and least preferred knowledge areas for both the industry and public sector participants. Our findings show that the most interesting knowledge areas of all respondents were primarily technical in nature (Data Security, Connection Security, System Security), but Organisational Security was also reported. The least interesting knowledge areas were mostly non-technical in nature (Human Security, Organisational Security, Societal Security) but also Component Security was reported. We also enquired about the preferred team size. The majority of the respondents preferred a team size of three to four persons. The preferred single session duration was 46–60 minutes. The results help cybersecurity professionals to match their knowledge needs with the existing cybersecurity proposition and to determine the right and most beneficial training for them. The results also assist the providers of cyber training and other exercises to describe the targeted development of specific cybersecurity and other knowhow in a coherent, standard-like, way.

**Keywords:** Cybersecurity, Cyber Range, Cyber Exercise, Capture-The-Flag, Skills

#### 1. Introduction

One of the most valuable assets in cybersecurity is the knowhow of the people. In a workplace, this naturally relates to the staff members. In addition to the global lack of competent cyber security experts (Blažič, 2021), there is a distinct gap between the appropriate skills of the cyber security professionals and the cyber security requirements of the occupations they hold (Nurse et al., 2021). For this, one of the goals in the Cyber Security for Europe (CyberSec4Europe) project was to specify learning objectives and competences required to develop and enhance cybersecurity skills for different profiles and roles. Considering the development and enhancing of skills of the workforce, there is a need not only to improve academic education but also the effectivity of hands-on courses. Cybersecurity exercises are one of the most effective modes for training the required skills and knowhow in the cybersecurity domain, especially under a stressful cyber-attack situation. Cybersecurity exercises arranged in cyber ranges enable organisations to be trained for reacting in situations when their assets or the whole organisation are experiencing cybersecurity incidents.

The Flagship 1 exercise, organised in January 2021 in connection with the CyberSec4Europe project, was an online cyber exercise. It featured the technical federation of cyber ranges so that participants in multiple locations across Europe could use the environment, which gathered positive feedback from the short after-survey (Kokkonen et al., 2023). The exercise this article focuses on, Flagship 2, was organised in January 2022. It focused on protecting the operations of a fictional train operator by offering (i) a cybersecurity exercise and (ii) an open external cyber security analyst activity using Capture-the-Flag (CTF) concepts (Kokkonen et al., 2022).

Both cybersecurity exercises and CTF challenges are useful tools in teaching cybersecurity topics. Firstly, the organisational aspects of cyber exercises have been studied in addition to the more traditional technical ones. Karjalainen et al. (2022) emphasise the evolution of cybersecurity exercises into organisational learning experiences. They conducted a survey on learning during an on-line exercise aimed at an organisation's various

work roles. Furthermore, Karjalainen and Kokkonen (2020) have proposed cyber arenas as learning environments to simulate organisations' environments to further their learning goals. According to them, this expansive use of cyber exercises provides "core knowhow elements of the cyber environment" for successful organisational exercises. Secondly, Capture-the-Flag (CTF) exercises are a well-known method of teaching cybersecurity in a class environment. The participants are presented with challenges related to cybersecurity, usually in a competitive setting (Mirkovic and Peterson, 2014). Using CTFs in cyber ranges for risk estimation shows that the combination is useful in many applications (Di Tizio et al., 2020). However, it seems that non-technical aspects should be included so that all the stakeholders could take part in exercises (Švábenský et al., 2021).

The importance of measuring learning should be highlighted when developing cyber exercises. Web questionnaires before and after a cyber exercise have been identified as useful tools to measure the experience of the exercise participants (Karjalainen et al., 2020). Using self-assessment questionnaires before an exercise is useful when setting learning objectives for an exercise (Vykopal et al., 2017). Their usage has been demonstrated to be a useful way to gather information before and after an exercise to evaluate learning outcomes (Vielberth et al., 2021).

The immediate feedback of Flagship 2 has been analysed by Kokkonen et al. (2022). The questionnaire was short and aimed to map out the participants' experiences and opinions about the usefulness of the exercise. The main finding is that the participants indicated that they obtained new skills.

In this article, we describe and analyse the results of the implemented Flagship 2 cyber exercise preliminary survey, which was designed by Karinsalo et al. (2022). The objective was to collect information from the registered participants prior to the exercise. This information consisting of more detailed information about the participants' background, expertise and interest areas could then be used to customise the exercise to better match the expectations and interests of the participants. The scientific contribution of this article comprises the results from the survey and the first analysis with the objective to provide meaningful activities for future cyber exercises through customisation. We selected the following research questions to guide our work:

1. How can we improve the quality of a cyber-exercise through pre-assessment of the participants?
   - How can we enhance the participant experience within a specific cyber-exercise?
2. What are the most and least interesting topics in a cyber-exercise?
3. How do the cyber-exercise needs of academia and research differ from the needs of industry?

The article is structured as follows. We begin the second chapter by describing the methodology. This includes the cyber exercise selected as the target for our work as well as the questionnaire generation, survey invitation and the analysis processes of the initial results. The third chapter focuses on the survey results and the analysis of data, providing the answers to our research questions. Finally, in chapter four we discuss the most significant findings from the survey and potential differences of our results when compared to previous research as well as ideas for future research before concluding the article in chapter five.

## 2. Methods

Flagship 2 consisted of two parallel activities. The primary activity was the cyber exercise that used a cyber range, a prepared complex learning environment. The exercise participants were placed into teams and coached by a dedicated team coach, who guided the team with questions. The exercise was targeted at CyberSec4Europe affiliates. The secondary activity was a capture-the-flag (CTF) exercise, where the participants were offered six digital samples or evidence exported from the exercise environment. The CTF activity was open for everyone. The participants of the CTF activity worked independently analysing the samples in a virtual machine with the focus on digital forensics. Later in this article, we refer to the CTF participants as *analysts*. Both activities required registration and lasted for two consecutive days. The participants were not scored nor otherwise assessed to avoid unnecessary competition, and thus a safe and comfortable environment for learning was created.

In order to define the cybersecurity skill levels of the participants prior to the exercise, as well as determine their expectations for it, we conducted a survey with six background questions and six research questions. We have described the survey and process thoroughly in Karinsalo et al. (2022), but the following paragraphs will summarise the survey content and process briefly.

The first part of the survey consisted of background questions such as participant email address (question #1), which was needed to identify the participants for after-survey purposes (not covered in this article). This was followed by background questions consisting of multiple-choice answers and covering the participants'

educational background (question #2), primary sector of the participant organisation (question #3), knowledge (question #4) and technical skill levels (question #5) related to cybersecurity exercises/hackathons, and the primary job role of the participant (question #6).

The second part of the survey introduced six research questions related to the cybersecurity exercise. This part covered the primary knowledge area development/improvement that the participant was interested in (question #7), preferred role within the exercise (question #8), ideal number of participants in the exercise teams (question #9) and preferred average length of the exercise sessions (question #10). The last two questions inquired about the knowledge area that the participant was least interested in (question #11), and there was an open question for any thoughts that the participant might have regarding the exercise (question #12).

We conducted the survey for the live exercise participant group during the timespan of January 11 – 28, 2023, and an identical survey for the analyst group during the timespan of January 19 – 24. The exercise hosts sent survey links in an invitation email sent to registered participants of both participant groups of the cyber exercise, and both surveys were conducted using the Questback online survey service (available at https://www.questback.com/). None of the survey questions were mandatory: respondents answered to as many questions as they chose.

The analysis was carried out by cross tabulation using the Microsoft Excel spreadsheet program. The answers to the questions were compared within and between categories. The respondents were divided into three categories. The category "Industry" included participants from companies in multiple domains while "Public sector" included participants from education, research, government, church, and non-profit organisations. The third category was used for respondents who did not disclose their organisation.

## 3. Results

### 3.1 Results from the survey process

The total number of surveyed participants was 82, consisting of live exercise participants and analysts. We received a total of 55 responses, yielding a response rate of 67%. Since the survey form, survey process and invitations were identical in both target groups, we have merged both groups into one respondent group. Two out of 55 respondents chose not to disclose their educational background, and nine respondents chose not to disclose their business sectors. Consequently, the analysis below excludes these respondents, resulting in 53 in the analysis concerning exercise participant education, and 46 in the analysis of their respective business sectors. However, we have included the non-disclosed as an independent group when calculating, e.g., responses by business sector.

### 3.2 Background data from the survey

The first background question covered the educational background of the participants. The most common educational background in total was Master's Degree (EQF7) with 20 respondents (37.7% out of 53), Bachelor's Degree (EQF6) with 19 respondents (35.8%) was quite close to the previous, and the third most common education was Doctoral Degree (EQF8) with 9 respondents (17%), Vocational education was fourth with 4 respondents (7.5%), and one respondent specified "Upper secondary school" in the open text field as their educational background (2%), which is quite similar to one of the available options, namely Vocational education (EQF4).

The second background question covered the business sector of the participants. The survey response data was minimised to include three business sector options: Industry, Public Sector, and an option to not to disclose the information. Industry was reported by 25 respondents (54% out of 46), and 21 respondents (46%) reported public sector as their home organisation's business sector. The split between exercise and CTF participants by business sector is shown in Table 1.

**Table 1: Responses split by Business sector between analysts and exercise participants.**

| Business Sector | Analysts | Exercise | Total |
|---|---|---|---|
| Industry | 16 | 9 | 25 |
| Public Sector | 5 | 16 | 21 |
| Not Disclosed | 6 | 3 | 9 |

| Business Sector | Analysts | Exercise | Total |
|---|---|---|---|
| Total | 27 | 28 | 55 |

The participants' knowledge level, including the understanding of concepts and types in cybersecurity exercises and hackathons was enquired in the third background question. The most common selected option was Intermediate (Apply/Analyse) with 26 respondents (47.2%, when $n$=55), Entry level (Remember/Understand) with 25 (45.5%), and Expert (Evaluate/Create) with four respondents (7.2%).

The fourth background question covered respondents' self-opinion of their technical skill level (e.g., usage of operating systems and IT environments, etc.) regarding cybersecurity exercises and hackathons (Table 2). The revised Bloom's taxonomy (Anderson et al., 2001) was used when categorising questions three and four.

**Table 2: Technical skill level by analysts and exercise participants**

| Technical skills level | Analyst | Exercise | Total |
|---|---|---|---|
| Entry level (Remember/Understand) | 7 | 11 | 18 |
| Intermediate (Apply/Analyse) | 18 | 13 | 31 |
| Expert (Evaluate/Create) | 2 | 4 | 6 |
| **Total** | **27** | **28** | **55** |

The fifth background question covered the participants' job role. The single-choice options followed the NIST - National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (Newhouse et al., 2017) categorisation. Two respondents reported a job role outside of the NICE framework (Table 3). In total 11 respondents did not disclose their job role.

**Table 3: Job roles reported by analysts and exercise participants**

| Job role | Analyst | Exercise | Total |
|---|---|---|---|
| Analyse (AN) | 1 | 6 | 7 |
| Investigate (IN) | 0 | 4 | 4 |
| Operate and Maintain (OM) | 9 | 3 | 12 |
| Oversee and Govern (OV) | 6 | 5 | 11 |
| Protect and Defend (PR) | 2 | 3 | 5 |
| Securely Provision (SP) | 2 | 1 | 3 |
| Communications | 0 | 1 | 1 |
| Teaching and research | 0 | 1 | 1 |
| Not disclosed | 7 | 4 | 11 |
| **Total** | **27** | **28** | **55** |

## 3.3 Research results from the survey

The research survey questions topics were (i) most interesting knowledge area to improve or develop, (ii) role to proceed in the interesting knowledge areas, (iii) ideal number of participants for the exercise teams, (iv) ideal duration of the exercise situation before the situation develops, and (v) least interesting knowledge area to improve or to develop. These are presented in the next paragraphs.

### *3.3.1 Most interesting knowledge areas*

Survey question #7 was multiple-choice, where the respondents were guided to select from one to three most interesting knowledge area options that the respondent was most interested in developing or improving during the exercise. The respondents were informed that the goals, and thus the contents of the Flagship exercise and CTF events were already set.

The nine knowledge area options offered in static order to the respondents have been presented in Table 4. Table columns are Public Sector (PS), Industry (I), and "I prefer not to disclose this information" (ND).

In total System Security was voted 36, Data Security 29, and Connection Security 23 times. Public sector and industry respondents voted System Security 16, and Data Security 14 times. Both Human Security and Organisational Security were voted eight times. Analyst respondents voted System Security 15 times. Connection and Data security were both voted 11 times.

**Table 4: Number of selected most interested knowledge area options**

| Knowledge area | Exercise | | | Analyst | | | Total |
|---|---|---|---|---|---|---|---|
| | PS | I | ND | PS | I | ND | |
| Data Security | 9 | 5 | 1 | 1 | 10 | 3 | 29 |
| Software Security | 5 | 2 | 2 | 3 | 6 | 1 | 19 |
| Component Security | 0 | 2 | 1 | 0 | 0 | 0 | 3 |
| Connection Security | 6 | 2 | 0 | 4 | 7 | 4 | 23 |
| System Security | 9 | 7 | 1 | 4 | 11 | 4 | 36 |
| Human Security | 5 | 3 | 1 | 0 | 3 | 3 | 15 |
| Organisational Security | 4 | 4 | 1 | 2 | 5 | 2 | 18 |
| Societal Security | 3 | 1 | 1 | 0 | 1 | 1 | 7 |
| Operate and maintain | 2 | 0 | 1 | 1 | 1 | 0 | 5 |
| **Total** | **43** | **26** | **9** | **15** | **44** | **18** | **155** |

### *3.3.2 The role to develop in Flagship 2*

The single choice question #8 surveyed the primary role that the respondents wanted to develop, by choosing the most interesting knowledge area options. The question followed the Newhouse et al., (2017) categorisation. Exercise participants selected Securely Provision (SP) nine (32.1%, $n$=28) times, and Investigate (IN) six (21.4%) times. Analysts selected seven times (25.9%, $n$=27) both Operate and Maintain (OM), and Securely Provision (SP).

**Table 5: Role to develop by selected knowledge areas**

| Role to develop | Exercise | | | Analyst | | | Total |
|---|---|---|---|---|---|---|---|
| | PS | I | ND | PS | I | ND | |
| Analyse (AN) | 3 | 2 | 1 | 1 | 3 | 1 | 11 |
| Investigate (IN) | 2 | 1 | 1 | 0 | 5 | 2 | 11 |
| Operate and Maintain (OM) | 2 | 1 | 0 | 3 | 0 | 0 | 6 |
| Oversee and Govern (OV) | 4 | 1 | 0 | 0 | 2 | 1 | 8 |
| Protect and Defend (PR) | 4 | 4 | 1 | 0 | 5 | 2 | 16 |
| Securely Provision (SP) | 0 | 0 | 0 | 1 | 0 | 0 | 1 |
| Collect and Operate (CO) | 1 | 0 | 0 | 0 | 1 | 0 | 2 |
| **Total** | **16** | **9** | **3** | **5** | **16** | **6** | **55** |

### *3.3.3 Ideal number of participants in an exercise team*

In question #9 we asked about the ideal number of participants for the exercise teams (Table 6). This was a single choice question. Exercise participants selected the option "3-4 participants" 19 (67.9%, $n$=28) times, and "more than six" seven (25.0%) times. Analysts selected the option "3-4 participants" 20 (74.0%, $n$=27) times.

Table 6: Ideal number of participants in an exercise team

| Number of participants | Exercise | | | Analyst | | | Total |
|---|---|---|---|---|---|---|---|
| | PS | I | ND | PS | I | ND | |
| 1–2 | 0 | 1 | 1 | 0 | 1 | 1 | 4 |
| 3–4 | 12 | 5 | 2 | 4 | 12 | 4 | 39 |
| 5–6 | 4 | 3 | 0 | 0 | 1 | 1 | 9 |
| more than 6 | 0 | 0 | 0 | 1 | 2 | 0 | 3 |
| **Total** | **16** | **9** | **3** | **5** | **16** | **6** | **55** |

### 3.3.4 *Exercise session development*

Cyber security exercises may have phases or sessions that develop either behind the scenes or in a way that is visible to the participant. In the single choice question #10 we asked the preferred session duration (Table 7). Exercise respondents selected the option "46-60 minutes" 11 (39.2%, $n$=28), and option "31-45 minutes" 10 (35.7%) times. Analysts reported "46-60 minutes" 13 (48.1%, $n$=27) and option "61-90 minutes" seven (25.9%) times.

Table 7: Exercise session duration

| Session duration | Exercise | | | Analyst | | | Total |
|---|---|---|---|---|---|---|---|
| | PS | I | ND | PS | I | ND | |
| 16-30 minutes | 2 | 0 | 0 | 1 | 1 | 0 | 4 |
| 31-45 minutes | 5 | 4 | 1 | 0 | 3 | 1 | 14 |
| 46-60 minutes | 6 | 4 | 1 | 3 | 9 | 1 | 24 |
| 61-90 minutes | 2 | 1 | 1 | 0 | 3 | 4 | 11 |
| more than 90 minutes | 1 | 0 | 0 | 1 | 0 | 0 | 2 |
| **Total** | **16** | **9** | **3** | **5** | **16** | **6** | **55** |

### 3.3.5 *Least interesting knowledge area*

Question #11 was similar to the question #7 but asking the opposite preference, i.e. the least preferred knowledge area development or improvement options. The respondents were guided to select from one to three options.

The exercise participants voted both Human Security and Societal Security nine times (Table 8). Component security was voted eight times. Data Security, and System Security, and Operate and maintain were each voted seven times. Analysts voted Societal Security 11, Organisational Security 10 times. Both Human Security, and Component Security were voted seven times.

Table 8: Number of selected least interesting knowledge area options

| Knowledge area | Exercise | | | Analyst | | | Total |
|---|---|---|---|---|---|---|---|
| | PS | I | ND | PS | I | ND | |
| Data Security | 4 | 3 | 0 | 1 | 2 | 1 | 11 |
| Software Security | 2 | 0 | 0 | 0 | 1 | 1 | 4 |
| Component Security | 4 | 2 | 2 | 1 | 4 | 2 | 15 |
| Connection Security | 2 | 1 | 1 | 0 | 3 | 1 | 8 |
| System Security | 3 | 3 | 1 | 0 | 0 | 0 | 7 |
| Human Security | 5 | 4 | 0 | 2 | 4 | 1 | 16 |
| Organisational Security | 2 | 2 | 0 | 1 | 6 | 3 | 14 |
| Societal Security | 5 | 4 | 0 | 4 | 6 | 1 | 20 |
| Operate and maintain | 5 | 2 | 0 | 0 | 3 | 2 | 12 |
| **Total** | **32** | **21** | **4** | **9** | **29** | **12** | **107** |

#### 3.3.6 *Open Question*

Question #12 was an open question to enquiry the respondents' thoughts about the forthcoming event. We received 11 responses. These responses are not covered in this article.

### 3.4 Findings

Our findings show that the most interesting knowledge areas reported by all respondents were primarily technical in nature (Data Security, Connection Security, System Security), but Organisational Security was also reported. The least interesting knowledge areas were mostly non-technical in nature (Human Security, Organisational Security, Societal Security) but included also Component Security.

Key data from the public sector or industry respondents are shown below.

Exercise participants ($n$=25):

- Ideal number for participants for the exercise teams = 3-4 (68.0%)
- Average exercise session (or phase) duration = 46-60 minutes (44.0%) or 31-45 minutes (40.0%)
- Most interesting knowledge development area = System security (16 votes), Data security (14 votes)
- Least interesting knowledge development area = Societal (9 votes) and Human security (9 votes).

Analysts ($n$=21):

- Ideal number for participants for the exercise teams = 3-4 (76.1%)
- Average exercise session (or phase) duration = 46-60 minutes (61.9%) or 61-90 minutes (33.3%)
- Most interesting knowledge development area = System (15 votes) and Connection (11) and Data security (11)
- Least interesting knowledge development area = Societal security (10 votes), Organisational security seven, and Human security six votes

Among industry partners, the least interesting topic was societal security. It covers cybercrime, law, policy, and privacy topics. Understanding of societal security is needed when establishing organisation's (cyber) security controls, procedures, and guidelines, and when responding to changing legislation requirements. The requirements are transformed to company's internal (cyber) security or privacy requirements, which are then handled and implemented in the organisation's way.

Among industry partners, human security and organisational security are the most diverging. Human security includes, e.g., identity management, social engineering, awareness and understanding, and usable security and privacy. What comes to end-users, awareness and understanding are key concepts. They are hoped e.g., not-to-fall into phishing emails or CEO frauds. Social engineering has been, even lately, successfully used as the mechanism to attack organisations. When such vulnerabilities in human security are exploited, then organisational security functions will activate, e.g., in the form of business continuity and incident management.

## 4. Discussion and future research

The information gained from this survey shows that the use of pre-assessment questionnaires in cybersecurity exercises can be a valuable source of information about the interests and needs of the participants. Especially with remote participation, a questionnaire can provide deeper understanding of their needs, and this way direct the development of future exercises with new requirements. Such requirements include areas of interests and pacing of the exercise.

The preference of technical hands-on exercises could be explained by the profile of the respondents. Moreover, the use of cyber exercises to improve organisational readiness could be a distant and unfamiliar topic to technically minded participants. Consequently, we should not draw the conclusion that organisational exercises are useless or unwanted in general. Based on our experience, even the most diverging elements, societal security and human security can be offered to specialists, managers, and directors in an exercise. Participants' reflection sessions after an exercise may raise the question whether the participant's organisation could detect or respond to the cyberattacks similarly or more efficiently than in the exercise, which could eventually improve the organisation's (cyber) security.

Both industry and public sector respondents found societal security the least interesting topic. This finding contrasts with Budde et al. (2023), who stated that societal values are interesting especially among industry

respondents in the cybersecurity context. This is most likely a result from different survey target groups, which in our case consist of people that had already declared their interest in a cyber exercise by completing the registration process, while the survey by Budde et al. was targeted to a broader group of cybersecurity experts in Europe. Since Budde et al. did not report detailed information about the respondent profiles, we can assume that their target group, more than ours, may have represented people from management-level personnel and thus been oriented to wider aspects of cybersecurity than ours.

As a conclusion, it could be that preconceptions of CTF events causes the technical aspect being seen as the most important part of the exercise.

The order of choices in the questionnaire could cause bias towards the first options. With larger numbers of respondents, randomized order of questions might provide a more balanced set of answers.

As the above discussion shows, there are still open questions in the motivation of cyber exercise participants. Further verification of the difference in interests in technical and societal knowledge is needed. Future research could also include an analysis of questionnaires during and especially after an exercise.

## 5. Conclusion

Our results display that a pre-assessment can (help to) improve the quality of a cyber exercise. The organisers will be able to profile the participants before the exercise and adjust the profiles to be as useful as possible to them. By asking about the expectations of the participants beforehand, the organisers can identify potential challenges. Knowing the participants' professional experience can also facilitate matching the skill level of the tasks to their skills.

The participant experience can be enhanced by creating tasks that fit the participants' profiles. The exercise roles can be distributed among the participants more effectively so that exercise participants and analyst positions are filled with suitable candidates. The preference for group size can also be considered, but the organisers should also use their own experience for optimal learning outcomes.

This study identified the three most interesting topics in a cyber exercise: System Security, Data Security and Connection Security. The least interesting topics were Societal Security, Human Security, Organisational Security and Component Security, the last two getting the same number of votes. When inspecting the differences between the Industry and Public Sector categories, both preferred System Security, Data Security, Connection Security. However, there were some differences between the categories: Industry also included Organisational Security in the top selection, while Public Sector contained also Software Security as a preference.

There were similarities between the Industry and Public Sector categories. Both listed Societal Security as the least preferred topic. In addition, Human Security was among the three least favourites. Curiously, the Industry respondents voted Organisational Security to be among both the most and the least preferred topics. Such polarisation could originate from the diverse work roles that the participants hold in their organisations. In the future, it could be beneficial to ask for just one top preference from the participants to reduce noise and to obtain hard preferences.

## Acknowledgement

This research was partially supported by the Cyber Security Network of Competence Centres for Europe (CyberSec4Europe) project funded by the European Union under the Horizon 2020 SU-ICT-03-2018 Programme Grant Agreement No. 830929.

The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript.

### References

Anderson, L., Krathwohl, D. R., Airasian, P. W., Cruikshank, K. A., Mayer, R. R., Pintrich, P. R., Raths, J. and Wittrock, M. C. (eds.) (2001) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives, abridged edition, Addison Wesley Longman, New York.

Budde, C., Karinsalo, A., Vidor, S., Salonen, J. and Massacci, F. (2022) "Consolidating cybersecurity in Europe – A case study on job profiles assessment", *Computers & Security*. https://doi.org/10.1016/j.cose.2022.103082

Di Tizio, G., Massacci, F., Allodi, L., Dashevskyi, S. and Mirkovic, J. (2020) "An experimental approach for estimating cyber risk: a proposal building upon cyber ranges and capture the flags", *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, pp. 56–65. https://doi.org/10.1109/EuroSPW51379.2020.00016

Blažič, B. J. (2021). "The cybersecurity labour shortage in Europe: Moving to a new concept for education and training", *Technology in Society*. Vol. 67, Art. 101769. https://doi.org/10.1016/j.techsoc.2021.101769

Karinsalo, A., Saharinen, K., Päijänen, J. and Salonen, J. (2022) "Pedagogical and self-reflecting approach to improving the learning within a cyber exercise", *Proceedings of the 21st European Conference on Cyber Warfare and Security, ECCWS 2022*. Vol. 21, No. 1, pp. 105–114. https://doi.org/10.34190/eccws.21.1.221

Karjalainen, M., Puuska, M. and Kokkonen, T. (2020) "Measuring Learning in a Cyber Security Exercise", *2020 12th International Conference on Education Technology and Computers (ICETC'20)*, pp. 205–209. https://doi.org/10.1145/3436756.3437046

Karjalainen, M. and Kokkonen, T. (2020). "Comprehensive Cyber Arena; the Next Generation Cyber Range", *Proceedings of the 5th IEEE European Symposium on Security Privacy Workshops, Virtual Event, 7–11 September 2020*. https://doi.org/10.1109/EuroSPW51379.2020.00011

Karjalainen, M., Kokkonen, T. and Taari, N. (2022). "Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise", Lehto, M. and Neittaanmäki, P. (eds.) *Cyber Security: Computational Methods in Applied Sciences*. Springer, Cham. https://doi.org/10.1007/978-3-030-91293-2_2

Kokkonen, T., Päijänen, J. and Sipola, T. (2022) "Multi-National Cyber Security Exercise, Case Flagship 2", *2022 14th International Conference on Education Technology and Computers (ICETC 2022)*. Forthcoming 2022. https://doi.org/10.1145/3572549.3572596

Kokkonen, T., Sipola, T., Päijänen, J. and Piispanen, J. (2023) "Cyber Range Technical Federation: Case Flagship 1 Exercise", Dimitrakos, T., Lopez, J., Martinelli, F. (eds.) *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*. Advanced Sciences and Technologies for Security Applications. Springer, Cham, pp. 1–13. https://doi.org/10.1007/978-3-031-16088-2_1

Mirkovic, J. and Peterson, P. (2014) "Class Capture-the-Flag Exercises", *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE '14)*.

Newhouse, W., Keith, S., Scribner, B. and Witte, G. (2017) *National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework*. NIST SP 800-181. Gaithersburg, MD: National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-181

https://doi.org/10.6028/NIST.SP.800-181

Nurse, J., Adamos, K., Grammatopoulos, A. and Di Franco, F. (2021) "Addressing the EU cybersecurity skills shortage and gap through higher education", European Union Agency for Cybersecurity (ENISA), https://www.enisa.europa.eu/publications/addressing-skills-shortage-and-gap-through-higher-education

Švábenský, V., Čeleda, P., Vykopal, J. and Brišáková, S. (2021) "Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges", *Computers & Security*, Vol. 102, Art. 102154. https://doi.org/10.1016/j.cose.2020.102154

Vielberth, M., Glas, M., Dietz, M., Karagiannis, S., Magkos, E. and Pernul, G. (2021) "A Digital Twin-Based Cyber Range for SOC Analysts", *Data and Applications Security and Privacy XXXV. DBSec 2021*. Lecture Notes in Computer Science. Vol. 12840. Springer, Cham, pp. 293–311. https://doi.org/10.1007/978-3-030-81242-3_17

Vykopal, J., Vizvary, M., Oslejsek, R., Celeda, P. and Tovarnak, D. (2017) "Lessons learned from complex hands-on defence exercises in a cyber range", *2017 IEEE Frontiers in Education Conference (FIE)*. https://doi.org/10.1109/FIE.2017.8190713

## Appendix 2. Cyber Range and Training and Learning Search Query

The URLs below can be used to replicate the search queries used in the literature review.

1. IEEE Xplore

   https://ieeexplore.ieee.org/search/searchresult.jsp?action=search&matchBoolean=true&queryText=(%22Abstract%22:%22Cyber%20Range%22%20AND%20(%22Abstract%22:%20%22learning%22%20OR%20%22Abstract%22:%20%22training%22))&highlight=true&returnType=SEARCH&matchPubs=true&refinements=ContentType:Conferences&refinements=ContentType:Journals&returnFacets=ALL&ranges=2022_2023_Year

2. Elsevier ScienceDirect

   https://www.sciencedirect.com/search?qs=%22cyber%20range%22%20AND%20%28learning%20OR%20training%29&date=2022-2023&articleTypes=REV%2CFLA&lastSelectedFacet=articleTypes

3. Google Scholar

   https://scholar.google.com/scholar?q=%22cyber+range%22+training+OR+learning&hl=fi&as_sdt=0,5&as_ylo=2022&as_yhi=2023&as_rr=1

## Appendix 3. Concept Map Propositions as Text

Note: save the table below as a tab separated .csv file. It is then possible to import into CMapTools via the path “File / Import / Propositions as Text”.

| | | |
|---|---|---|
| Technical platform | May have many | Domain specific system |
| An event in a Cyber Range | may have many | Attendee role |
| Technical platform | may have many | Workstation |
| Reactive | may be kind | Defensive |
| Technical platform | may have many | Server |
| Workstation | is connected by | Network |
| Green team (GT) member | is kind of | Passive attendee |
| Passive attendee | may be | Human |
| An event in a Cyber Range | may have many | Cyber Range |
| Cyber Arena | has one or more | Cyber Range |
| Access time | may be | Continuous |
| Operating system (OS) | is kind of | Software |
| Content | may be | Reusable |
| Reusable | may impelement | Operational Federation (CROF) |
| Content | may have many | Proactive |
| Proactive | may be kind | Defensive |
| An event in a Cyber Range | has | Access time |
| Competition | is kind of | Event type |
| Domain specific system | is connected by | Network |
| Physical | may be | Temporary |
| Online | may be | Temporary |
| Testing | is kind of | Event type |
| Workstation | may have many | Software |
| Patient monitor | is kind of | Domain specific system |
| Technical platform | has | Functionalities |
| Location | may be | Online |
| Computer virus | is kind of | Software |
| Respirator | is kind of | Domain specific system |
| An event in a Cyber Range | has | Content |
| Server | may have many | Software |
| Cyber Range | may have many | Location |
| Access time | may be | Predetermined |
| Active attendee | may be | Human |
| Technical federation (CRTF) | may be | Permanent |
| Content | may have many | Operative |
| Observer | is kind of | Passive attendee |
| Technical federation (CRTF) | is kind of | Interoperability |
| Interoperability | is one of | Capability |
| Technical platform | may have many | Location |
| Passive attendee | is one of | Attendee role |

| | | |
|---|---|---|
| An event in a Cyber Range | Is accessible from | Location |
| Physical | may be | Permanent |
| Domain specific system | may have many | Software |
| Proactive | may be kind | Offensive |
| Online | may be | Permanent |
| Ethical hacking | is kind of | Offensive |
| Cyber Range | has one or more | Technical platform |
| Technical federation (CRTF) | may have many | Technical platform |
| Education | is kind of | Event type |
| An event in a Cyber Range | has | Lifecycle |
| Cerfication | is kind of | Event type |
| Technical federation (CRTF) | may be | Temporary |
| An event in a Cyber Range | may have many | Event type |
| Server | is connected by | Network |
| Exercise | is kind of | Event type |
| Technical platform | has | Features |
| Active attendee | may be | Software |
| Technical platform | has | Capacity |
| Reactive | may be kind | Operative |
| Training | is kind of | Event type |
| Passive attendee | is one of | Active attendee |
| Technical platform | has one or more | Network |
| Operational Federation (CROF) | is kind of | Interoperability |
| Content | may have many | Reactive |
| Passive attendee | may be | Software |
| Technical platform | has | Capability |
| Location | may be | Physical |

## Appendix 4. Hints to Article Licences

The table below contains hints, which occurrence in a web page could have indicated the authors access to the content, either licensed or open access, or no access. Contents were copy-pasted from a Python dict() instance.

| No access | Licenced or open access |
|---|---|
| "does not subscribe to this content" | "Access provided by" |
| "This is a preview of subscription content" | "Under a Creative Commons license" |
| "Chapter Preview" | "Under a Creative Commons" |
| "Section snippets" | "You have full access to this open access article" |
| "Buy Instant PDF Access" | "Creative Commons" |
| "Purchase PDF" | "Open Access" |
| "Access via your institution" | |
| "Add to cart" | |
| "Access through your institution" | |
| "Get Access" | |
| "Buy Chapter" | |
| "Snippet" | |