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