Multi-National Cyber Security Exercise, Case Flagship 2

TERO KOKKONEN, Institute of Information Technology, JAMK University of Applied Sciences, Finland
JANI PÄIJÄNEN, Institute of Information Technology, JAMK University of Applied Sciences, Finland
TUOMO SIPOLA, Institute of Information Technology, JAMK University of Applied Sciences, Finland

Cyber security is not merely about securing devices and focusing on software and hardware. Staff members with skills and know-how are among the most valuable assets in the context of cyber security. Globally, there is a lack of competent cyber security experts available and cyber security skills should be educated more widely. One of the most effective practices for training cyber security experts is a cyber security exercise. During a cyber security exercise, the learning audience train their skills with a realistic scenario depicting a hectic and stressful cyber incident or cyber attack. In order to successfully implement a cyber security exercise, there must be sufficient technical infrastructure mimicking required systems and networks. The infrastructure should allow the use of realistic threat actors with realistic attack vectors and real malware without compromising any production environments. Facilities offering such infrastructure are widely known as the cyber ranges. There are two special requirements raised by modern cyber range exercises: (i) cyber range collaboration, including capabilities for sharing and pooling cyber range services, and (ii) on-line cyber security exercises without restrictions of being on-site on the exercise premises. The requirement of implementing on-line exercises has increased especially after the spread of COVID-19 pandemic. In this study, we introduce Flagship 2, a multinational state-of-the-art on-line cyber security exercise based on cyber range federation. We analyse the technical implementation of the cyber range federation and the learning outcomes of the exercise event based on a participant survey and relevant theories. The analysed results are explained with identified future research topics.

CCS Concepts: • **Security and privacy → Human and societal aspects of security and privacy**; • **Networks → Network services**; • **Applied computing → Interactive learning environments**.

Additional Key Words and Phrases: Cyber Security, Cyber Range, Cyber Arena, Cyber Security Exercise, Distance Learning, Learning Environments, Technical Federation

ACM Reference Format:
Tero Kokkonen, Jani Päijänen, and Tuomo Sipola. 2022. Multi-National Cyber Security Exercise, Case Flagship 2. In *ICETC 2022: 2022 14th International Conference on Education Technology and Computers, October 28–30, 2022, Barcelona, Spain.* ACM, New York, NY, USA, 10 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Cyber domain is an extremely complex field to handle and requires special skills and know-how. Two of the most valuable assets in cyber security is the know-how of individuals and the know-how of the organisation, especially when reacting and making decisions under the hectic and stressful situation of a cyber incident. One should train and exercise regularly in order to obtain, manage and upgrade that skillset. The best way to enhance cyber security skills of an individual or an organisation is a cyber security exercises. There should be appropriate technical infrastructure for arranging a cyber security exercise. An instance of such infrastructure is called a cyber range.

There are several different cyber ranges implemented for special purposes. Actually, because the sampling of the different cyber ranges is so heterogeneous and there are infrastructures with different purposes and different scales, paper [12] proposed the term *Cyber Arena* to describe comprehensive, large scale cyber security infrastructures intended for research, development, training and exercises. Chouliaras et al. conducted a systematic survey including different cyber ranges to examine the key components and tools of the cyber ranges [1]. The wide range of cyber

ICETC 2022, October 28–30, 2022, Barcelona, Spain
2022. https://doi.org/10.1145/nnnnnnn.nnnnnnn

ranges has led to the requirement of cyber range federation for sharing and pooling the existing cyber range capabilities.

In our earlier study [16], we analysed the Flagship 1 exercise organised on 12–13 January 2021 [22]. The objective of the earlier Flagship 1 exercise was to prove technical federation capability. In other words, the use case study demonstrated that cyber range federation can be implemented, and that the federated multi-national cyber security exercise can be conducted using this implementation. The earlier study identified the next phases of the research with the concluding words [16]: *"the first version of the cyber range technical federation forms a good foundation for the next phase of the implementation, which will be showcased during the Flagship 2 exercise in January 2022."* The Flagship 2 exercise was organised on 25–26 January 2022 [10]. This paper will describe and draw conclusions about the Flagship 2 exercise, including analysis based on the participant questionnaire.

The rest of the paper is organised as follows: First, the cyber range federation concept is described in Section 2. It is followed by Section 3 which illustrates the Flagship 2 exercise with its technical description. Section 4 describes the participant questionnaire, and the results are complemented with the analysis of the external activity as described in Section 5. Finally, the whole study is concluded with identified future work in the Section 6.

2 CYBER RANGE BASED EXERCISES AND CYBER RANGE FEDERATION

Cyber security is not merely implementation of secure systems; the main essence in the cyber security are well-trained system operators with the required skills and know-how [26]. Training of traditional technical engineering skills is usually based on hands-on training; the hands-on training in relevant technical infrastructure is useful and effective for skills required with cyber security [14, 28]. For gaining the effective learning during the cyber security exercise, paper [23] introduce a non-linear cyber security exercise concept allowing 'Branching/Forking', 'Fast Forward', 'Playback', and 'Pause-Adapt-Repeat' of scenario, events and injects in the exercise. There are several different exercise scenarios required in the different exercises with different objectives. In that sense, Wen et al. proposed ontology-based scenario development for cyber security exercises [30], and authors of paper [19] introduce a 10-step process for exercise organisation. In the complex cyber domain, coherent situational awareness is extremely important to be maintained because situational awareness forms basics for decision making. Cyber range based exercises are effective for training the maintaining of cyber security situational awareness and for training the decision making based on that maintained situational awareness [4].

Globally, there is wide interest in cyber range infrastructures and there are several cyber ranges implemented by universities, research centres, governmental agencies and private industry sector actors. Xu et al. conducted a research on cyber ranges and found 1763 cyber range related articles released between 2001-2020 from the Web of Science [31]. Cyber ranges are often specialised in one certain sector or perspective. For example, paper [9] introduces a cyber range for cyber security training of maritime ports. Quite often, there are limited capabilities to simulate complex cross-sector interconnections of the cyber domain; in that sense it is reasonable to share the capabilities between different cyber ranges as a cyber range federation [20]. The idea of pooling and sharing of capabilities is well-known in the defence cooperation and for example European Defence Agency (EDA) has a released concept of pooling and sharing [6]. Actually EDA's first Cyber Defence Pooling & Sharing Project about cyber range federation was showcased already in 2019 [7]. Across the four pilot programs of European Cybersecurity Competence Network, the Cyber Range Focus Group (CRFG) has been constituted for promoting the European cyber range ecosystem [2, 27]. In a wider perspective, the cyber range federation is not just sharing and pooling of capabilities, but the federation also offers the capability to organise virtual on-line cyber security exercises for wider learning audience without limitations of on-site events. Especially during the COVID-19

pandemic, training events that are classically conducted on-site are forced to be transformed to virtual on-line events [25]. That requirement of on-line exercises also catalyses the need for cyber range federations. Learning results during the on-line cyber security exercise are studied in the paper [13] and it can be concluded that the learning objectives can be achieved by implementing the on-line cyber security exercise, and overall, a cyber security exercise serves as an excellent teaching platform and a tool for diverse cyber domain.

Furthermore, the scoring of the learning audience during the exercise event is a double-edged sword. It can convert learning audiences' behaviour and decision making towards optimising the scoring. In our exercises, as in the Flagship 2 exercise, the scoring is not used for guarantee that the learning audience are not afraid to make mistakes. However, as part of the gamification, the scoring can motivate the learning audience. In their paper, Diakoumakos et al. introduced a gamification scoring model for cyber range federation exercises [5].

3 CASE FLAGSHIP 2

3.1 Exercise Scenario

The learning audience of the earlier Flagship 1 exercise was divided into five different blue-teams simulating individual Digital Forensic Investigation and Response (DFIR) teams of a fictional organisation known as University of Kybereo. Their main duty consisted of investigating and responding to cyber security incidents. The exercise narrative of Flagship 2 was that the participants were new cyber security employees of Cyber Rails s.r.l., a fictional Italian train operator. During their introduction, these new employees detected that there were anomalous activities in the monitored systems. Further analyses revealed that there was an active threat actor that had intruded the environment. According to the exercise scenario, the objective of the threat actor was lowering trustworthiness and the amount of train traveling and public transport usage. The motivation of the threat actor was to protest the high and rising costs of private motoring, especially the increased fuel costs. As a camouflage the threat actor activated a ransom on the master controller host, which was used to operate and monitor Cyber Rails' traffic management system. The threat actor also stole the Customer Relationship Management (CRM) database from Cyber Rails.

The learning objectives for the participating learning audience were:

- Understand that even modern security mechanisms, such as Trusted Platform Modules (TPMs), may have weaknesses that can be exploited.
- Understand how well integrated security controls and Security Information and Event Management (SIEM) can support performing a DFIR activities.
- Understand that performing DFIR activities requires resources and is time consuming in a large environment with more than 100 hosts and servers governed by security controls and SIEM.

Flagship 2 exercise had 19 participants from 10 European countries (see Table 1), representing 13 affiliates. These participants were placed into four blue-teams, each blue-team having equal tasks and a dedicated team coaches. The task of coaches was to support the participants using the tooling, and if necessary, providing guiding questions to the team. The exercise participants were not revealed the threat actor targets or motivation to simulate a real-world situation, for example, a cyber incident is detected, but it is yet unknown if the incident is an intended or unintended cause of action.

Compared to the previous Flagship 1 exercise, the threat actor in the Flagship 2 was more organised and more sophisticated. The threat actor of Flagship 1 was a single person, but in Flagship 2 the speed and the used techniques, tactics and procedures (TTPs) revealed that the threat actor was formed by a team of many individuals. For example, a malicious office document, an

Table 1. Countries of the Flagship 2 exercise participants.

Country #	Country	No. Persons	Percent of persons
1.	Estonia	1	5%
2.	Finland	2	11%
3.	Germany	2	11%
4.	Greece	1	5%
5.	Italy	5	26%
6.	Luxembourg	1	5%
7.	Slovenia	2	11%
8.	Spain	1	5%
9.	Sweden	3	16%
10.	United Kingdom	1	5%
Total	10	19	100%

obfuscated PowerShell script, a custom ransomware and custom (simulated) on-train firmware were used. While the earlier Flagship 1 had contents for organisation's technical specialists, privacy (GDPR) specialists and managerial roles, due to the technical difficulty level and relatively short exercise duration, Flagship 2 included only technical specialist participant roles.

3.2 Open External Cyber Security Analyst Activity

As an extra sidetrack, Flagship 2 included an open parallel activity for external cyber security analysts. The analysts were required legal age and earlier experience of Linux command line usage, being an entry level analyst activity [3]. The analysts were offered and ordered to use a prepared virtual machine, created by Masaryk University's Cyber SandBox Creator [28]. The virtual machine is freely accessible from GitLab repository [17]. The analysts were offered a technical support forum as a guidance with the virtual machines. No support was offered to the analysis of the actual samples. The scenario consisted of a simulated cyber security service provider as a customer and the individual analyst (participant) as a service provider for that customer. Due to the nature of the event, all the samples to be analysed were immediately available for download.

3.3 Technical Implementation of the Flagship 2 Exercise

The overall technical infrastructure of Flagship 2 was based on the Cyber Arena called RGCE (Realistic Global Cyber Environment) [11]. Flagship 2 used predefined requirements for the cyber range technical federation [16, 24], and the technical solution of the federation was based on the technical implementation of Flagship 1 exercise [16, 21, 22]. During the Flagship 2 exercise, a participant's access to the cyber arena was covered as illustrated in the Fig. 1. As seen in the figure, the core technical solution was based on open-source SD-WAN technology, published by ZeroTier Inc. [32].

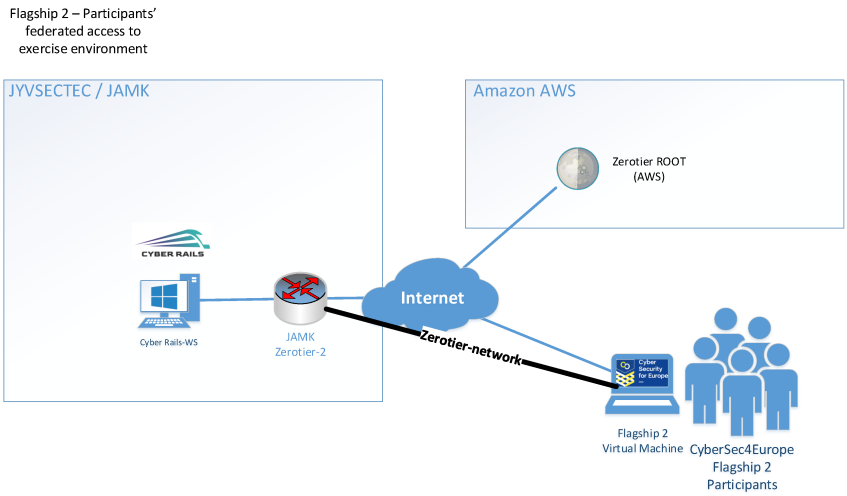

Fig. 1. Flagship 2 federation network overview.

In the Flagship 2 exercise, all the exercise related servers and workstations were located in the in-premises network of the organisation, that differs from the Flagship 1 where some of the services were located in a federated Amazon AWS network. The organisational environment of Cyber Rails included logical network blocks for datacenter, track side and Traffic control center as shown in Fig. 2. In total there were more than 100 servers and workstations dedicated for the Flagship 2 exercise.

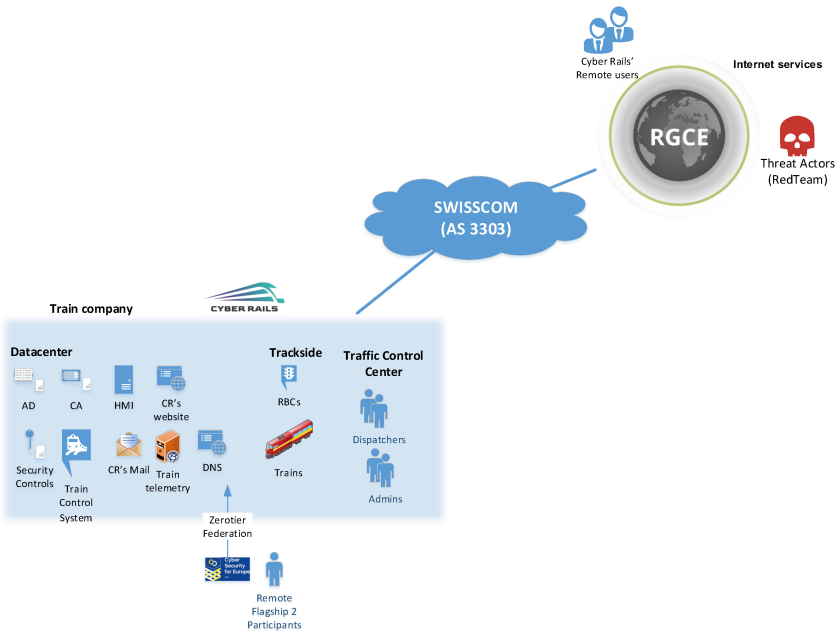

Fig. 2. Overview of the Flagship 2 exercise environment.

4 PARTICIPANT QUESTIONNAIRE

4.1 Questionnaire Description

The participants were asked about their experience and the usefulness of the exercise afterwards. The questionnaire was carried out using the Webropol platform [29]. The participants were made aware of the use of the answers for research when registering for the exercise. The terms of service and the privacy policy of the project state: "*The learning experiences and gathered data from this event will be used in research and development.*" There were 21 registrations, and 19 of the registered participated in the exercise. The survey was sent to the participants immediately after the active phase of the exercise but before the feedback session, and they were given 15 minutes to answer the questionnaire.

The questionnaire contained yes/no questions and free text questions. In addition, one question was a selection of pre-defined values. The questions, their types and the number of responses are shown in Table 2. The number of the surveyed participants was $N = 19$, and the number of those who answered to the survey was $n = 15$, meaning that 79% of participants answered the questionnaire. Some questions in the questionnaire were answered by all the participants but especially the free text questions were not answered by all of them. Even though the number is small, these results give an indication about the usefulness of this type of exercise through qualitative analysis.

Table 2. Questions, their types and answer rates.

Question	Type	n
1. Your team in the exercise?	selection	15
2. What are your feelings now?	free text	13
3. Did you find the exercise beneficial for you?	yes/no	15
4. Please describe how?	free text	13
5. Did you learn something new?	yes/no	15
6. Please describe what?	free text	12
7. Would you recommend Flagship 2 for a friend or a colleague?	yes/no	15
8. Free feedback about Flagship 2	free text	9

4.2 Answer Analysis

Question 1. As can be seen in the Fig. 3, we received responses from each participating team. The teams are equally represented in the answers, as expected. This indicates that each team had adequate participation in the exercise and felt that giving feedback was meaningful.

Question 2. All the free text responses about initial feelings reported positive emotions about participating. Other things that received thanks were the facilitators, good first experience in an exercise, learning about operations and security and the exercise environment.

Question 3. All the participants answered "Yes" to the question "Did you find the exercise beneficial for you?"

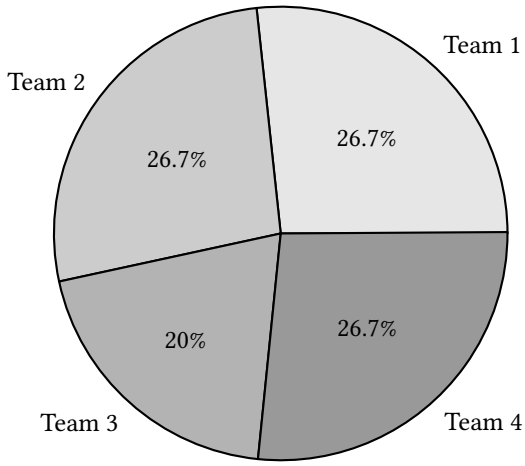

Fig. 3. Distribution of teams to which the respondents belonged, $n = 15$.

Question 4. When asked about how they found the exercise beneficial, the participants described the following major topics:

- Learning new skills,
- learning about cyber security operations,
- working in a blue-team defending against cyber attacks,
- importance of logging and tools related to it,
- experiencing an environment that resembles real life, and
- better understanding the big picture.

Question 5. When asked "Did you learn something new?", 100% of the respondents answered with the option "Yes", the other option being "No".

Question 6. The free text answers indicate that the participants learned about new tools such as command line, security information and event management systems (SIEM) and firewalls. Even if a participant was familiar with some of the tools, there were other areas that they learned about.

Question 7. The question "Would you recommend Flagship 2 for a friend or a colleague?" resulted in the same 100% approval.

Question 8. Free feedback showed that the remote environment received positive comments, as did the team facilitators. However, the participants had had some difficulty understanding the usefulness of some tools. There were some connection issues that had been a problem for some of the participants. In general, the answers took a positive stance about the scenario and how the exercise was organised.

4.3 Discussion

The findings support theories of learning linked to research focusing on cyber ranges. This relates to the theory of andragogy for adult learners, in which adults are mostly self-directed and capable of fusing new practical impulses with prior learned knowledge [15, 18]. This method of learning has been shown to be useful in the cyber range context [13, 14]. The authentic learning theory presumes that stimulation of learning and transmitting the learned to working life tasks can be

enabled by an authentic learning environment [8]. A cyber range can act as such an environment, enabling learning of cyber security skills and operating procedures [12, 13].

As a summary of the results from this and the previous exercise [16], it can be said that both the Flagship 1 and the Flagship 2 exercises were successful when it comes to disseminating knowledge and practices. They implemented a continuation of state-of-the-art technical cyber range federation that supported both technical progress and learning outcomes of the participating learning audience, including significant participant satisfaction.

5 EXTERNAL OPEN CYBER SECURITY ANALYST ACTIVITY

There were $N = 61$ registrations in total as external cyber security analysts for the exercise but 18 of them did not submit any solutions, which leaves $n = 43$ persons who participated as external analysts. As with the participant questionnaire, the participants were made aware that the solutions could be used in research and development during the registration. There were six assignments, and the participants could try to submit their solutions as many times as they wanted until they were correct. As can be seen in Table 3, 44% of the participants solved all six assignments, 60% solved at least five and 72% solved at least four. In conclusion, most of the assignments were at the correct difficulty level for most of the participants.

Table 3. Distribution of correct solutions.

Correct solutions	Participants with that many correct solutions	Percentage
6/6	19	44%
5/6	7	16 %
4/6	5	12 %
3/6	2	5 %
2/6	4	9 %
1/6	2	5 %
0/6	4	9 %
Total:	43	100 %

6 CONCLUSION

Cyber security exercises are one of the most impressive resources for training cyber security experts. In this study, we showcased the on-line cyber security exercise called Flagship 2. In addition, the state-of-the-art technical implementation of the cyber range federation was studied and implemented. Flagship 2 exercise was the continuation of a series of cyber security exercises. The first exercise, Flagship 1, was a proof-of-concept for the federation capability, while Flagship 2 utilised that concept with the objective of learning during the exercise. Consequently, Flagship 2 created a comprehensive multinational on-line cyber security exercise based on federated cyber range capabilities.

The analysed participant survey reveals that the technical implementation is effective as a platform for such an exercise. The scenario, including the events and inputs, supports learning outcomes from the learning audience's perspective. The questionnaire indicates participant satisfaction and them obtaining new skills. Furthermore, the external analyst assignments show that such challenges

can be tailored to a previously unknown audience. The scenario is also in line with the relevant theories related to adult learning and hands-on learning using authentic learning environments.

As a future topic, the sharing and pooling concept should be studied more extensively. Moreover, organisational learning during the cyber security exercise versus learning of an individual expert should be studied.

ACKNOWLEDGMENTS

This research is funded by *Cyber Security Network of Competence Centres for Europe (CyberSec4Europe)* project of the Horizon 2020 SU-ICT-03-2018 program. The authors thank colleagues at Masaryk University for implementing the virtual machines used in the external analyst assignments. The authors would like to thank Ms. Tuula Kotikoski for proofreading the manuscript.

REFERENCES

[1] Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. 2021. Cyber Ranges and TestBeds for Education, Training, and Research. *Applied Sciences* 11, 4 (2021). https://doi.org/10.3390/app11041809

[2] Cyber Competence Network. n.d.. Cyber Range Focus Group. https://cybercompetencenetwork.eu/focus-groups/cyber-range-focus-group/. Accessed: 8 February 2022.

[3] CyberSec4Europe. 2021. JAMK To Conduct Flagship 2: An Online Cybersecurity Exercise Activity. https://cybersec4europe.eu/jamk-to-conduct-flagship-2-an-online-cybersecurity-exercise-activity/. Accessed: 22 February 2022.

[4] Thibault Debatty and Wim Mees. 2019. Building a Cyber Range for training CyberDefense Situation Awareness. In *2019 International Conference on Military Communications and Information Systems (ICMCIS)*. 1–6. https://doi.org/10.1109/ICMCIS.2019.8842802

[5] Jason Diakoumakos, Evangelos Chaskos, Nicholas Kolokotronis, and George Lepouras. 2021. Cyber-Range Federation and Cyber-Security Games: A Gamification Scoring Model. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 186–191. https://doi.org/10.1109/CSR51186.2021.9527972

[6] European Defence Agency, EDA. 2013. EDA's Pooling & Sharing -factsheet. https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s_30012013_factsheet_cs5_gris. Accessed: 7 February 2022.

[7] European Defence Agency, EDA. 2019. EDA Cyber Ranges Federation project showcased at demo exercise in Finland. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/11/07/eda-cyber-ranges-federation-project-showcased-at-demo-exercise-in-finland. Accessed: 7 February 2022.

[8] Jan Herrington and Ron Oliver. 2000. An instructional design framework for authentic learning environments. *Educational Technology Research and Development* 48, 3 (01 Sep 2000), 23–48. https://doi.org/10.1007/BF02319856

[9] Olivier Jacq, Pablo Giménez Salazar, Kamban Parasuraman, Jarkko Kuusijärvi, Andriana Gkaniatsou, Evangelia Latsa, and Angelos Amditis. 2021. The Cyber-MAR Project: First Results and Perspectives on the Use of Hybrid Cyber Ranges for Port Cyber Risk Assessment. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 409–414. https://doi.org/10.1109/CSR51186.2021.9527968

[10] JAMK University of Applied Sciences, Institute of Information Technology / JYVSECTEC. 2021. Upcoming event: FLAGSHIP 2, an online cybersecurity exercise. https://jyvsectec.fi/2021/12/flagship-2/. Accessed: 7 February 2022.

[11] JAMK University of Applied Sciences, Institute of Information Technology / JYVSECTEC. n.d.. RGCE Cyber Arena. https://jyvsectec.fi/rgce. Accessed: 7 February 2022.

[12] Mika Karjalainen and Tero Kokkonen. 2020. Comprehensive Cyber Arena; The Next Generation Cyber Range. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroSi&PW)*. 11–16. https://doi.org/10.1109/EuroSPW51379.2020.00011

[13] Mika Karjalainen, Tero Kokkonen, and Niko Taari. 2022. *Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise.* Springer International Publishing, Cham, 43–57. https://doi.org/10.1007/978-3-030-91293-2_2

[14] Mika Karjalainen, Samir Puuska, and Tero Kokkonen. 2020. Measuring Learning in a Cyber Security Exercise. In *2020 12th International Conference on Education Technology and Computers* (London, United Kingdom) *(ICETC'20)*. Association for Computing Machinery, New York, NY, USA, 205–209. https://doi.org/10.1145/3436756.3437046

[15] Malcolm S Knowles. 1995. *Designs for adult learning: Practical resources, exercises, and course outlines from the father of adult learning.* American Society for Training and Development, Alexandria, VA.

[16] Tero Kokkonen, Tuomo Sipola, Jani Päijänen, and Juha Piispanen. 2022. Cyber Range Technical Federation: Case Flagship 1 Exercise. (2022). Chapter accepted to be published in a book of Springer, Cham.

[17] Masaryk University. 2022. Flagship2-sandbox. https://gitlab.fi.muni.cz/cybersec/cs4e/flagship2-sandbox. Accessed: 23 February 2022.
[18] Sharan B Merriam and Laura L Bierema. 2013. *Adult learning: Linking theory and practice.* John Wiley & Sons.
[19] Sten Mäses, Kaie Maennel, Mascia Toussaint, and Veronica Rosa. 2021. Success Factors for Designing a Cybersecurity Exercise on the Example of Incident Response. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 259–268. https://doi.org/10.1109/EuroSPW54576.2021.00033
[20] Nikos Oikonomou, Notis Mengidis, Minas Spanopoulos-Karalexidis, Antonis Voulgaridis, Matteo Merialdo, Ivo Raisr, Kaarel Hanson, Paloma de La Vallee, Theodora Tsikrika, Stefanos Vrochidis, and Konstantinos Votis. 2021. ECHO Federated Cyber Range: Towards Next-Generation Scalable Cyber Ranges. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 403–408. https://doi.org/10.1109/CSR51186.2021.9527985
[21] Juha Piispanen and Jani Päijänen. 2021. Evaluation report on integration demonstration. https://cybersec4europe.eu/wp-content/uploads/2021/08/D7.3-Evaluation-report-on-integration-demonstration-v1.3_submitted.pdf.
[22] Jani Päijänen, Jarmo Viinikanoja, and Juha Piispanen. 2021. Flagship 1. https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf.
[23] Florian Skopik and Maria Leitner. 2021. Preparing for National Cyber Crises Using Non-linear Cyber Exercises. In *2021 18th International Conference on Privacy, Security and Trust (PST)*. 1–5. https://doi.org/10.1109/PST52912.2021.9647795
[24] Elina Suni, Juha Piispanen, Jarmo Nevala, Jani Päijänen, and Karo Saharinen. 2020. Report on existing cyber ranges, requirements. 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.
[25] Kee Hock Tan and Eng Lieh Ouh. 2021. Lessons Learnt Conducting Capture the Flag CyberSecurity Competition during COVID-19. In *2021 IEEE Frontiers in Education Conference (FIE)*. 1–9. https://doi.org/10.1109/FIE49875.2021.9637404
[26] Vincent E. Urias, William M.S. Stout, Brian Van Leeuwen, and Han Lin. 2018. Cyber Range Infrastructure Limitations and Needs of Tomorrow: A Position Paper. In *2018 International Carnahan Conference on Security Technology (ICCST)*. 1–5. https://doi.org/10.1109/CCST.2018.8585460
[27] Csaba Virág, Jakub Čegan, Tomáš Lieskovan, and Matteo Merialdo. 2021. The Current State of The Art and Future of European Cyber Range Ecosystem. In *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*. 390–395. https://doi.org/10.1109/CSR51186.2021.9527931
[28] Jan Vykopal, Pavel Čeleda, Pavel Seda, Valdemar Švábenský, and Daniel Tovarňák. 2021. Scalable Learning Environments for Teaching Cybersecurity Hands-on. In *2021 IEEE Frontiers in Education Conference (FIE)*. 1–9. https://doi.org/10.1109/FIE49875.2021.9637180
[29] Webpropol Oy. n.d.. Webropol - Lead With Information. https://webropol.com/. Accessed: 23 February 2022.
[30] Shao-Fang Wen, Muhammad Mudassar Yamin, and Basel Katt. 2021. Ontology-Based Scenario Modeling for Cyber Security Exercise. In *2021 IEEE European Symposium on Security and Privacy Workshops (EuroS PW)*. 249–258. https://doi.org/10.1109/EuroSPW54576.2021.00032
[31] Quan Xu, Congwang Kong, Ming Xian, Jian Liu, Ziyuan Li, and Guangyu Chen. 2021. Cyber Range Research Based on Scientific Knowledge Map. In *2021 International Conference on Computer Technology and Media Convergence Design (CTMCD)*. 133–137. https://doi.org/10.1109/CTMCD53128.2021.00036
[32] ZeroTier Inc. n.d.. ZeroTier Global - Area Networking. https://www.zerotier.com/. Accessed: 23 February 2022.