Cyber Range Technical Federation: Case Flagship 1 Exercise

Tero Kokkonen, Tuomo Sipola, Jani Päijänen, Juha Piispanen

Abstract Modern cyber domain is an extremely complex field to master. There are numerous capricious dependencies between networked systems and data. In cyber security, technology has a major role, but the knowledge and skills of the individuals combined with the incident response processes of the organisations are even more important assets. Those assets foster the cyber resilience of the organisation. The most effective ways to uphold these urgent assets are training and exercising. Cyber security exercises in particular have proven their efficiency in improving cyber security skillsets. During the cyber security exercises, it is possible to train cyber defence and incident response manoeuvres in stressful and hectic situations of being under cyber attack or intrusion. To achieve the capability to organise technical cyber security exercises with real attacks and real malware, technical training infrastructure mimicking real networks and systems is required. Such infrastructures are universally called cyber ranges or cyber arenas. Globally, cyber security exercises have become more common during the last decade, and there are several cyber ranges with diverse capabilities. Pooling and sharing the capabilities of cyber ranges raises the requirement to establish a cyber range technical federation. In this paper, a state-of-the-art implementation of the cyber range technical federation is introduced. In addition, the implementation demonstrated and evaluated during the Flagship 1 on-line cyber security exercise is discussed.

Key words: Cyber Security, Cyber Range, Cyber Arena, Cyber Security Exercise, Technical Federation

Institute of Information Technology, JAMK University of Applied Sciences, Jyväskylä, Finland
e-mail: {tero.kokkonen,tuomo.sipola,jani.paijanen,juha.piispanen}@jamk.fi

This is an author accepted manuscript version. The original appeared as: Tero Kokkonen, Tuomo Sipola, Jani Päijänen and Juha Piispanen. "Cyber Range Technical Federation: Case Flagship 1 Exercise." In: *Collaborative Approaches for Cyber Security in Cyber-Physical Systems*. Ed. by Theo Dimitrakos, Javier Lopez and Fabio Martinelli. Advanced Sciences and Technologies for Security Applications. Cham, Switzerland: Springer, 2023, pp. 1–13. DOI: 10.1007/978-3-031-16088-2_1

1 Introduction

The modern cyber domain is extremely complex and includes complicated structures of networks and dynamic interactions of networked computer systems added with a increasing amount of potentially encrypted data. Understanding that entity requires special skills and awareness. Learning and experiencing during the cyber security exercises is an unquestionable fact. A well known quote attributed to general George S. Patton illustrates the fact quite aptly: *"You fight as you train."* The importance of cyber security exercises is noticed in several national and international official documents. The EU's Cybersecurity Strategy for the Digital Decade [10] states that at the EU level awareness and exercises should enhance cyber defence capabilities and total cyber resilience, whereas Finland's Cyber Security Strategy [31] announces that both national and international exercises are utilised for ensuring the required high level education in the critical cyber competence. The importance of exercising is also noted in the proposal for a directive of the European Parliament and of the Council on the resilience of critical entities [11].

For achieving the capability to organise comprehensive cyber security exercises with modern vulnerabilities, attack vectors and malware, the total cyber domain shall be mimicked. For cyber security exercising, a cyber range can be understood parallel to a traditional shooting range that is serving competence to exercise skills with weapons, operations or tactics [36]. A cyber range shall implement a technical platform with the capability to simulate the required networks and systems for supporting the training & exercises (and also research & development activities) in the cyber domain. Cyber range is a centrally controlled environment including the required systems, tools and networks combined with a realistic Internet simulation, user simulation and background traffic generation. As a closed environment, cyber range offers risk-free usage of modern and realistic threat environments including real malware, attacks and intrusions [23, 26, 25, 17].

European Cyber Security Organisation (ECSO) defines a cyber range as follows [12]: *"A cyber range is a platform for the development, delivery and use of interactive simulation environments."* They elaborate that a simulation environment represents organisation's ICT, OT, mobile and physical systems, applications and infrastructure. Such an environment could include simulation of attacks, users and their activities. Other simulated services, listed by them, could include Internet, public and third-party services. Furthermore, ECSO describes [12]: *"A cyber range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases."*

Overall, there are many diverse cyber ranges implemented by security authorities, research centres, universities or industry all over the globe [37]. The requirements and perspective of cyber range development are often limited to specific use cases or capabilities, and therefore existing cyber ranges fluctuate from laboratory based test beds to tremendous virtual exercise arenas that mimic structures of the real global Internet. Cyber ranges are used for several objectives: as a platform for research, development and testing activities and also as an infrastructure for training and exercise

transactions. For example, Deckard introduces a cyber-electromagnetic range executing kinetic and non-kinetic activities [5], while CyFRS is a fast recoverable cyber range based on a real environment [40]. He et al. introduce usage of cyber range for electricity grid as part of critical infrastructure [19], while Chen et.al reflect on the construction of a cyber range for personnel training in power information system [2]. Shangting and Quan discuss an industrial sector cyber range adopting QEMU-IOL virtualization technology [32]. Paper [6] proposed an approach for estimating the risk of compromise based on the data available from cyber ranges. Authors of[4] described the usage of cyber range for training the situational awareness in cyber defence. Authors of [38] reviewed in their position paper requirements for cyber ranges exploring the National Cyber Range (NCR) as a blueprint. Human-computer interaction, such as user interface, visualisation, design patterns and gamification, is also a concern when designing cyber ranges [33]. Lately, there have been activities to list existing cyber ranges. As a deliverable of Cyber Security for Europe project [3], the report on existing cyber ranges based on survey conducted across Europe has been released [34], and also the FORESIGHT project has produced a review of cyber ranges and test beds [37].

As illustrated above, the spectrum of cyber ranges and their usage are extremely heterogeneous. Karjalainen and Kokkonen introduce the concept of Cyber Arena (CA) for describing cyber range with the capability to simulate the total cyber domain including unexpected dependencies [23]. The different capabilities of cyber ranges have provoked the requirement for technical collaboration between different cyber ranges. Collaboration, pooling and sharing of capabilities in a cyber range federation enables an even wider compilation of cyber range capabilities.

In this paper, the implementation of cyber range technical federation is described and demonstrated during the Flagship 1 cyber security exercise, executed in January 2021 [21, 30]. The Flagship 1 exercise was executed as a remote, entirely on-line, exercise with participants from 22 affiliations from 15 different countries across Europe. The exercise showcased a cyber range technical federation using state-of-the art open-source Software-Defined Wide Area Network technology with great success. It is noticeable that compared to the on-site exercise, the on-line exercise has great challenges with exercise control functionalities, communication inside the Blue Team, communication between the Blue Teams and maintaining the situational awareness [24].

The rest of this paper is constructed as follows: the Section 2 describes the concept of cyber range federation. The Flagship 1 exercise with the description of technical requirements and implementation is illustrated in the Section 3. After that, in the Section 4, the results of participant questionnaire are analysed as the reliability assessment. Finally, results with found future research topics are concluded in the Section 5.

2 Cyber Range Federation

The basic requirement for a cyber range federation is quite obvious. The modern cyber domain is extremely complex, and different partners have different expertises. By the federation, those different expertises can be gathered and utilized. Several strategy papers indicate the requirement for co-operation in the cyber capabilities. For example, the National Cyber Strategy of the United States of America [35] indicates that partners have special cyber capabilities that can complement the existing ones. Also the EU's Cybersecurity Strategy for the Digital Decade [10] states the co-operation with international partners for strengthening the cyber defence capabilities.

Pooling & Sharing concept is noticed by both NATO and the EU. European Defence Agency (EDA) defines Pooling & Sharing as the EU concept which refers to increasing collaboration on military capabilities [13]. Smart Defence concept of NATO [27] includes Pooling & Sharing for generating cost-effective modern defence capabilities. A state-of-the-art example of Pooling & Sharing in the cyber domain is EDA's Cyber Defence Pooling & Sharing Project about Cyber Ranges Federation that showcased the technical co-operation and collaboration between different national cyber ranges at the European level [14, 15, 16].

The requirement for a cyber range federation is also noticed in the non-military domains. The EU launched four cyber security competence networking pilot projects [9], and all of those four projects have recognised the requirement for a cyber range federation. As stated by Graziano [18]: *"The idea behind a federation of cyber ranges is that multiple cyber ranges can be combined to provide greater simulation and scaling capabilities while leveraging on the vertical expertise of different cyber ranges."*

The cyber range federation can be either operational or technical [34]: *"Operational Federation can be achieved "offline", without integrating or performing any technical federation of cyber ranges. The technical federation of cyber ranges enables the federated parties to utilize or consume specified functionalities, services, capabilities or resources from another party or parties of the federation."* This paper focuses on the cyber range technical federation.

3 Case Flagship 1

The Flagship 1 exercise was conducted on 12-13 January 2021 as a unique on-line cyber security exercise available to partners of the CyberSec4Europe project [21, 30, 3]. The learning audience of the Flagship 1 exercise were from 22 affiliations across the Europe. During the exercise, the learning audience were placed into five different Blue Teams.

Blue Teams were simulating five individual Digital Forensic Investigation and Response (DFIR) teams of a fictional organisation known as University of Kybereo. The main task of DFIR teams was to investigate a response to a cyber security incident of the University of Kybereo. DFIR teams were using the provided inci-

dent response plans, communication guidelines, other documentation and required technical solutions. The roles of the learning audience were assigned based on the expertise queried prior to the Flagship 1 exercise [30].

The technical exercise environment was based on RGCE Cyber Arena [22]. Realistic Global Cyber Environment (RGCE) is a comprehensive cyber arena with substantial features. RGCE assembles in an isolated private cloud a realistic global world and real organization environments. RGCE implements thousands of virtual machines mimicking the global Internet and various organisation environments.

The objectives of the learning audience were to understand the DFIR process and team roles, technical investigation tools, communication within the team, within the organisation, its stakeholders and authorities. A hidden objective that was not exposed before or during the exercise was to understand the benefits of cyber security exercises for non security organisations. This objective was showcased to the learners by providing them incomplete incident response plans and communication guidelines. During the exercise they noticed incompleteness; however, they still had the main task to do, so the learning audience had to improvise. After the exercise, the provided documentation completeness was criticised. Actually, during the cyber security exercise an organisation may verify its processes, guidelines and documentation and after the exercise those can be further developed.

3.1 Technical Requirements of the Flagship 1 Cyber Range Federation

Technical specification and requirements of the implemented cyber range federation were based on the Piispanen's Master's Thesis [28]. In his thesis Piispanen introduces three different use cases for cyber range technical federation:

- **Networked cyber ranges** where different cyber ranges are connected to each other in a point-to-point, point-to-multipoint, or mesh-like manner for sharing the cyber range capabilities.
- **Extension of the cyber range's functionalities** where one cyber range serves as a provider (a hub) and offers connectivity to other cyber ranges that may provide additional functionalities to the hub.
- **Testbeds** where the cyber range offers domain-specific features such as testbeds or labs.

In the Flagship 1 exercises, the use case *"Testbeds"* was used. That use case is very similar to networked cyber ranges but in a smaller scale. The Master's Thesis did not cover the end user connectivity requirement and for this purpose, the remote end user connectivity use case was introduced in the Flagship 1 exercise. In addition to end user connectivity, the use case also specified the identification and the registration of users. The main requirements for the cyber range technical federation of the Flagship 1 were as follows [29, 34]:

- *"Specification 2.1: Overlay network SHALL support L3 connectivity into a cyber range (i.e. routed connectivity between cyber ranges)."*

- *"Specification 2.2: Overlay network SHOULD support L2 connectivity into a cyber range (i.e. extending L2 network between cyber ranges)."*
- *"Specification 2.3: Overlay interface SHALL support IPv4 and IPv6 connections in dual-stack."*
- *"Specification 2.4: Overlay network SHALL support IPv4 and IPv6 (cyber range Internetconnectivity does not need to be dual-stack)."*
- *"Specification 2.5: Overlay network SHALL support the following topologies: point-to-point, hub-and-spoke, partial-mesh and full-mesh."*
- *"Specification 2.6: Overlay network SHOULD support connectivity behind NAT/FW."*
- *"Specification 2.7: Overlay network endpoint SHOULD be implemented either in hardware or in virtual appliance."*
- *"Specification 2.8: End-to-End Round-Trip-Time (RTT) SHALL be less than 200ms."*
- *"Specification 2.9: Overlay network SHALL have centralized management to control interconnections between cyber ranges."*
- *"Specification 2.10: Centralized management SHOULD be available to all cyber ranges."*
- *"Specification 2.11: Overlay network SHALL support segregation of concurrent exercises."*
- *"Specification 2.12: Overlay network SHALL be encrypted using industry standard protocols."*

3.2 Technical Implementation of the Flagship 1 Cyber Range Federation

The cyber range technical federation was demonstrated during the Flagship 1 exercise. The cyber range technical federation was based on open-source Software-Defined Wide Area Network (SD-WAN) technology. SD-WAN was chosen based on the features of security and flexible deployment options. SD-WAN allows configuration modifications during the execution and it doesn't require complete preconfiguration as for example site-to-site Internet Protocol Security (IPSec) or Virtual Private Network (VPN) solutions which are commonly used for federation purposes. The chosen open-source SD-WAN technology was ZeroTier, developed and open-sourced by ZeroTier Inc [39].

The capability for participants remote connectivity to the exercise environment was established by the technical federation. By the technical federation, also the features and functionalities of the RGCE Cyber Arena were extended by running a number of contents harmoniously in the Amazon AWS cloud [1]. The high-level cyber range technical federation environment is illustrated in the Figure 1.

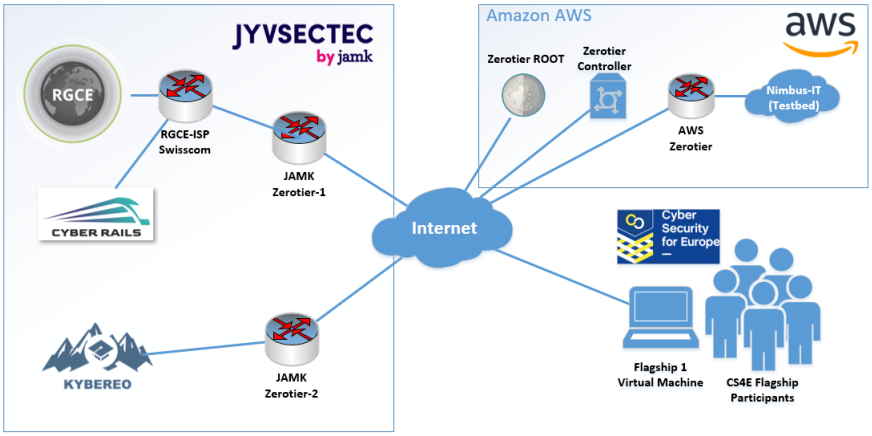

Fig. 1 Cyber range technical federation environment of the Flagship 1 exercise [29].

Cyber range technical federation environment of the Flagship 1 exercise included:

- ZeroTier SD-WAN infrastructure.
- Testbed, fictional cloud service provider that offered services to exercise organisations.
- Kybereon, Fictional University. The participants were part of the Kybereo's DFIR-team.
- Cyber rails, Fictional Train company. Partnership with Kybero.
- Swisscom and RGCE, Global internet functionalities and services.

The SD-WAN infrastructure of the technical federation was implemented on Amazon AWS cloud. ZeroTier Inc offers free public ZeroTier network, however a separated ZeroTier infrastructure on AWS was implemented. For the technical federation a SD-WAN edge router was deployed to AWS and to RGCE Cyber Arena. With these edge routers a secure network connection could be created between AWS and RGCE. A second edge router was also implemented. The second edge router was dedicated to remote users connectivity.

SD-WAN network controller was implemented because the infrastructure was disconnected from the Internet; thus the public Internet-connected ZeroTier's network controller could not be used. The developed controller used the JSON API of ZeroTier. Isolated networks can be created to the federation from that controller. The registration portal was implemented on top of our controller. When users was registered to our federation, the portal automatically added the end users as a member to their designated networks. A virtual machine image was created for the participant, which automatically connected to the federation network. The end users did not need to perform any configuration when they had the exercise's virtual machine, and the same virtual machine image was suitable for all participants because the configuration and network memberships were configured from our controller.

4 Reliability Assessment

A reliability assessment was conducted with a participant questionnaire during the final stages of the Flagship 1 exercise. The questionnaire was conducted anonymously without an indication of the respondent's identity or affiliation. When joining the exercise, the respondents were also informed about the usage of the provided data for scientific research and development of the environment in the privacy policy of the exercise. The questionnaire was conducted immediately after the technical part of the exercise to guarantee that the exercise audience had a strong emotion about it, and the experience was fresh in the participants' memories. As described earlier, there were participants from 22 affiliations across Europe. 21 individuals replied to the questionnaire. The questionnaire included closed yes/no questions and open questions for clarifying the feedback. Answers of the closed questions were analysed as quantitative data while answers of the open questions were processed by qualitative methods. First the answers of the open questions were coded (breakdown) [8] and then analysed by applying a qualitative content analysis [7, 20].

There were five Blue Teams in the exercise. The respondents of the questionnaire were distributed in the Blue Teams in accordance with Figure 2.

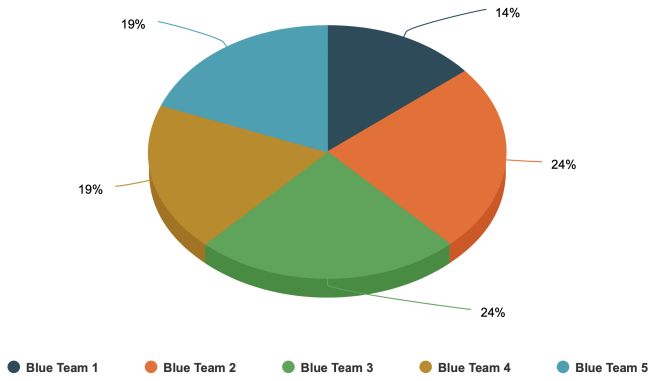

Fig. 2 Distribution of participants in Blue Teams.

The overall experience immediately after the Flagship 1 exercise was researched with the open question *"What are your feelings now?"*. All the answers were positive without any criticism for the cyber range technical federation or conducted exercise. Some quotations from the answers illustrate the participants' feelings:

> *"Very satisfied and excited. A really nice environment.", "Good, it was great learning experience.", "Superb platform, interesting scenario, good guidance.", "I found the exercise really interesting."*

There was also a closed yes/no question to find out whether the exercise was beneficial for the participants. All of the respondents indicated that the exercise was beneficial, which was clarified with the open question *"Please describe how?"*. Noticeable is that even though the exercise was conducted on-line, also the teamwork was indicated there. As an illustration, some quotations from the answers are listed as follows:

> *"It's a great way to learn.", "To learn the overall methodology and using new tools.", "Now I have idea on how these exercises really work.", "New tools and techniques + teamwork." "I was exposed to a very good cyber range."*

It was also queried with the closed yes/no question whether the participants learned something new during the Flagship 1 exercise; this was further clarified with the open question *"Please describe what?"*. As illustrated in Figure 3, one of the respondents (5%) indicated that they did not learn anything new, but all the others (95%) indicated that they had learned something new during the exercise. It is noticeable that there were no critical open comments about learning something new. Following quotations from the answers illustrate this:

> *"Learned a lot. The teamwork was perfect.", "Procedures, methodologies and teamwork around cyber security.", "Use of new tools."*

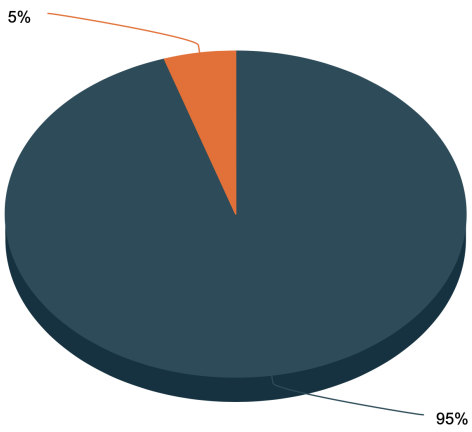

Fig. 3 Answers to the question "Did you learn something new?".

It was also investigated whether the participants would recommend such an exercise for their colleagues. All the answerers indicated positive recommendation of the exercise. Finally, there was an opportunity to give open feedback. Most of it was positive; however, there was criticism against on-line exercise compared to

an on-site exercise. Actually, such a feedback was predictable because communication during an on-line exercise is more challenging than communication on-site. Following quotations from the answers illustrate the feedback:

> *"It is a beautiful experience, very informative and fun.", "Very interesting and great fun.", "Keep up the good work! Waiting for the Flagship 2.", "Thanks for all attempts and environment. Exercise needs to be held physically, virtual experience is missing a lot!"*

Overall, it can be summarised that the implementation of cyber range technical federation was successful. Of course, there were some critics, but it was predictable because people are used to participating in on-site exercises, and an on-line exercise has its own challenges with communication processes and maintaining cyber security situational awareness inside the Blue Team. It is noticeable that this was the first version of the open-source solution and the first time to execute a pan-European on-line exercise with remote participants. In that sense, the results of the showcase were positive and form a great foundation for the Flagship 2 exercise conducted during the next year.

5 Conclusion

During this case study the implementation of cyber range technical federation was tested during the Flagship 1 on-line cyber security exercise. The technical implementation was based on state-of-the art open-source SD-WAN technology with great success, as it enabled the parties to join the on-line exercise. SD-WAN was chosen based on the features of security and flexible deployment options compared to, e.g., site-to-site IPSec or VPN solutions which are commonly used for federation purposes. It is noticeable that the on-line cyber security exercise is technically much more demanding than the on-site cyber security exercise because the learning audience of the exercise is located remotely across the globe. This raises requirements for the usability of the technical environment in order to create a satisfactory user experience. The on-line cyber security exercise has special challenges also with exercise control functionalities, communication inside the Blue Team, communication between the Blue Teams and maintaining situational awareness.

The Flagship 1 exercise demonstrated a good performance and capability of chosen state-of-the-art technologies and the implementation of cyber range technical federation was a success. A participant survey was conducted and analysed as a reliability assessment of the usefulness of the showcased environment. Closed questions of the participant survey were analysed as quantitative data while open questions of the participant survey were analysed by qualitative methods. As a summary, the analysis indicated that the participants were pleased with the exercise experience, and the technical implementation obtained positive feedback. In conclusion, the first version of the cyber range technical federation forms a good foundation for the next phase of the implementation during the Flagship 2 exercise in January 2022.

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

References

1. Amazon Web Services, Inc.: Amazon Web Services (AWS). https://aws.amazon.com/. Accessed: 8 April 2021
2. Chen, Z., Yan, L., He, Y., Bai, D., Liu, X., Li, L.: Reflections on the construction of cyber security range in power information system. In: 2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), pp. 2093–2097 (2018). DOI 10.1109/IAEAC.2018.8577685
3. Cyber Security Network of Competence Centres for Europe -project: Cyber Security for Europe (CS4E). https://cybersec4europe.eu/. Accessed: 7 April 2021
4. Debatty, T., Mees, W.: Building a cyber range for training cyberdefense situation awareness. In: 2019 International Conference on Military Communications and Information Systems (ICMCIS), pp. 1–6 (2019). DOI 10.1109/ICMCIS.2019.8842802
5. Deckard, G.M.: Cybertropolis: breaking the paradigm of cyber-ranges and testbeds. In: 2018 IEEE International Symposium on Technologies for Homeland Security (HST), pp. 1–4 (2018). DOI 10.1109/THS.2018.8574134
6. Di Tizio, G., Massacci, F., Allodi, L., Dashevskyi, S., Mirkovic, J.: An experimental approach for estimating cyber risk: a proposal building upon cyber ranges and capture the flags. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS PW), pp. 56–65 (2020). DOI 10.1109/EuroSPW51379.2020.00016
7. Drisko, J., Maschi, T.: Content analysis. Oxford University Press, New Yourk, NY (2016)
8. Elliott, V.: Thinking about the coding process in qualitative data analysis. The Qualitative Report **23**, 2850–2861 (2018)
9. European Commission: Four EU pilot projects launched to prepare the European Cybersecurity Competence Network. https://digital-strategy.ec.europa.eu/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network (2019). Accessed: 9 April 2021
10. European Commission: JOINT COMMUNICATION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL: The EU's Cybersecurity Strategy for the Digital Decade. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=JOIN:2020:18:FIN (2020)
11. European Commission: Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN (2020)
12. European Cyber Security Organisation (ECSO): Understanding Cyber Ranges: From Hype to Reality. https://www.ecs-org.eu/documents/uploads/understanding-cyber-ranges-from-hype-to-reality.pdf (2020)
13. European Defence Agency, EDA: EDA's Pooling & Sharing -factsheet. https://eda.europa.eu/docs/default-source/eda-factsheets/final-p-s_30012013_factsheet_cs5_gris. Accessed: 9 April 2021
14. European Defence Agency, EDA: Cyber ranges: Eda's first ever cyber defence pooling & sharing project launched by 11 member states. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2017/05/12/cyber-ranges-eda-s-first-ever-cyber-defence-pooling-sharing-project-launched-by-11-member-states (2017). Accessed: 7 April 2021
15. European Defence Agency, EDA: Cyber ranges federation project reaches new milestone. https://www.eda.europa.eu/info-hub/press-centre/latest-news/2018/09/13/cyber-ranges-federation-project-reaches-new-milestone (2018). Accessed: 7 April 2021

16. European Defence Agency, EDA: 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 (2019). Accessed: 7 April 2021
17. Ferguson, B., Tall, A., Olsen, D.: National cyber range overview. In: 2014 IEEE Military Communications Conference, pp. 123–128 (2014). DOI 10.1109/MILCOM.2014.27
18. Graziano, A.: About Federation of Cyber Ranges, Market Places and Technology Innovation. https://www.linkedin.com/pulse/federation-cyber-ranges-market-places-technology-almerindo-graziano/ (2020). Accessed: 9 April 2021
19. He, Y., Yan, L., Liu, J., Bai, D., Chen, Z., Yu, X., Gao, D., Zhu, J.: Design of information system cyber security range test system for power industry. In: 2019 IEEE Innovative Smart Grid Technologies - Asia (ISGT Asia), pp. 1024–1028 (2019). DOI 10.1109/ISGT-Asia.2019.8881739
20. Hsieh, H.F., Shannon, S.E.: Three approaches to qualitative content analysis. Qualitative Health Research **15**(9), 1277–1288 (2005). DOI 10.1177/1049732305276687
21. JAMK University of Applied Sciences, Institute of Information Technology: Coming soon – a cybersecurity exercise that emphasizes learning and cooperation. https://jyvsectec.fi/2021/01/cybersec4europe-projects-cybersecurity-exercise-on-january/ (2021). Accessed: 7 April 2021
22. JAMK University of Applied Sciences, Institute of Information Technology / JYVSECTEC: RGCE Cyber Arena. https://jyvsectec.fi/rgce. Accessed: 8 April 2021
23. Karjalainen, M., Kokkonen, T.: Comprehensive cyber arena; the next generation cyber range. In: 2020 IEEE European Symposium on Security and Privacy Workshops (EuroSi&PW), pp. 11–16 (2020). DOI 10.1109/EuroSPW51379.2020.00011
24. Karjalainen, M., Kokkonen, T., Taari, N.: Key Elements of On-Line Cyber Security Exercise and Survey of Learning During the On-Line Cyber Security Exercise, pp. 43–57. Springer International Publishing, Cham (2022). DOI 10.1007/978-3-030-91293-2_2. URL https://doi.org/10.1007/978-3-030-91293-2_2
25. National Institute of Standards and Technology NIST: Cyber Ranges. https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf. Accessed: 13 January 2020
26. Nevavuori, P., Kokkonen, T.: Requirements for training and evaluation dataset of network and host intrusion detection system. In: Á. Rocha, H. Adeli, L.P. Reis, S. Costanzo (eds.) New Knowledge in Information Systems and Technologies, pp. 534–546. Springer International Publishing, Cham (2019)
27. North Atlantic Treaty Organization, NATO: Smart Defence. https://www.nato.int/cps/en/natolive/topics_84268.htm (2017). Accessed: 9 April 2021
28. Piispanen, J.: Technical specification for federation of cyber ranges. Master's thesis, JAMK University of Applied Sciences (2018). URL http://urn.fi/URN:NBN:fi:amk-201812172201O
29. Piispanen, J., Päijänen, J.: Evaluation report on integration demonstration. https://cybersec4europe.eu/wp-content/uploads/2021/08/D7.3-Evaluation-report-on-integration-demonstration-v1.3_submitted.pdf (2021)
30. Päijänen, J., Viinikanoja, J., Piispanen, J.: Flagship 1. https://cybersec4europe.eu/wp-content/uploads/2021/06/D6.4-Flagship-1-v1.1-submitted.pdf (2021)
31. Secretariat of the Security Committee: Finland's Cyber security Strategy, Government Resolution 3.10.2019. https://turvallisuuskomitea.fi/wp-content/uploads/2019/10/Kyberturvallisuusstrategia_A4_ENG_WEB_031019.pdf (2019)
32. Shangting, M., Quan, P.: Industrial cyber range based on qemu-iol. In: 2021 IEEE International Conference on Power Electronics, Computer Applications (ICPECA), pp. 671–674 (2021). DOI 10.1109/ICPECA51329.2021.9362692
33. Shepherd, L.A., de Paoli, S., Conacher, J.: Human-computer interaction considerations when developing cyber ranges. International Journal of Information Security and Cybercrime **9**(2), 28–32 (2020). DOI 10.19107/IJISC.2020.02.04

34. Suni, E., Piispanen, J., Nevala, J., Päijänen, J., Saharinen, K.: 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 (2020)
35. The White House, signed by President Donald J. Trump: National Cyber Strategy of the United States of America. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf (2018)
36. Tian, Z., Cui, Y., An, L., Su, S., Yin, X., Yin, L., Cui, X.: A real-time correlation of host-level events in cyber range service for smart campus. IEEE Access **6**, 35,355–35,364 (2018). DOI 10.1109/ACCESS.2018.2846590
37. Ukwandu, E., Farah, M.A.B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., Bellekens, X.: A review of cyber-ranges and test-beds: Current and future trends. Sensors **20**(24) (2020). DOI 10.3390/s20247148
38. Urias, V.E., Stout, W.M.S., Van Leeuwen, B., Lin, H.: Cyber range infrastructure limitations and needs of tomorrow: A position paper. In: 2018 International Carnahan Conference on Security Technology (ICCST), pp. 1–5 (2018). DOI 10.1109/CCST.2018.8585460
39. ZeroTier Inc.: ZeroTier Global - Area Networking. https://www.zerotier.com/. Accessed: 29 April 2021
40. Zhang, Z., Lu, G., Zhang, C., Gao, Y., Wu, Y., Zhong, G.: Cyfrs: A fast recoverable system for cyber range based on real network environment. In: 2020 Information Communication Technologies Conference (ICTC), pp. 153–157 (2020). DOI 10.1109/ICTC49638.2020.9123273